第７章　米中サイバーセキュリティ交渉[1]

土屋　大洋

はじめに

「サイバー攻撃（cyber attack）」が国際法上の「攻撃」として認められるためには、人命への危害や物理的な破壊を伴わなければならないとされている[2]。しかし、現実には情報の抜き取りやサービス等の停止も含めて広義の「サイバー攻撃」が人口に広く膾炙している。その手法は日進月歩で進化しており、生物界のウイルスが環境に応じて適者生存を繰り返し、進化していくように、コンピュータ・ウイルスやマルウェアもまた、新たな防御策をかいくぐるために進化を繰り返している。生物界のウイルスとコンピュータのウイルスが違うのは、人間の意図による進化が行われているかどうかという点であろう。生物界のウイルスは遺伝子のロジックによって進化するが、コンピュータのウイルスはいまだ自動で進化する余地は小さく、そのプログラムないしコードを書き換える人間がいるからこそ進化している。

かつては、コンピュータ・ウイルスを書き換える人間は、興味本位や自己の技能の誇示のためにそれを行っていた。しかし、広義のサイバー攻撃が個人的な動機だけではなく、政治的・経済的・軍事的な動機を達成するための手段となるにつれ、より多くの多様な人間が関わるようになっている。ほとんどが個人のブラック・ハット（悪意のある）ハッカーによる試みだったウイルス作成は、組織的な試みとして行われるようになり、各国の軍隊が攻撃のためのツールとして行うようにもなっている。そうしたウイルスやマルウェア（悪意のあるソフトウェア）はブラックマーケットで誰でも金銭と引き替えに入手可能になっている。

対立の構図は、個人対個人、国家対国家といった単純なものではなく、個人、非政府／非営利組織、営利企業、国家、国家連合などがそれぞれ攻撃側・防御側に立つ複雑なものになりつつある。そして、攻撃者は多くの場合インターネットの雲の中に隠れているため、素性が分からないという「アトリビューション（帰属・属性）問題」を生み出し、対立軸すらはっきりしないという点で、問題をよりいっそう深刻にしている[3]。

攻撃対象を見ても、かつてはパーソナル・コンピュータやサーバーがほとんどだったが、IoT（Internet of Things）といわれる時代になり、いわゆる情報通信機器以外のものもネットワークにつながるようになり、サイバー攻撃の対象となりつつある。近年のニュースでは、飛行機や自動車を第三者が乗っ取ることができるとする報告もある[4]。

さらには、重要インフラストラクチャに対するサイバー攻撃（つまり狭義のサイバー攻撃）もまた実現性を帯びつつある。重要インフラストラクチャに対するサイバー攻撃の実例はいまだ数えるほどであり、そのうち実際に行われたことが政府機関によって公式に確認されたものは2010年のイランの核施設に対するスタックスネット（STUXNET）攻撃（イラン政府が攻撃を受けたことを確認[5]）、2014年のドイツの溶鉱炉に対する攻撃（ドイツ政府が攻撃を受けたことを確認したが詳細は不明[6]）にとどまっていた。しかし、2015年12月23日にウクライナ西部で140万世帯が停電になり、サイバー攻撃によるものではないかという疑いが強まっている[7]。

そして、将来においてはそうした狭義のサイバー攻撃が、金融部門、通信部門、運輸交通部門、あるいは防衛（軍事）部門などに対して行われる可能性は否定できない。そうしたサイバー攻撃は容易にサイバースペースの境界を越えた戦争にエスカレートする可能性があり、もはや看過することはできない。

その中で1つの大きな軸となるのが、米中の動向である。世界第1位と第2位の経済大国であり、両国はサイバーセキュリティをめぐって近年つばぜり合いを続けている。そして、もはや事務方が協議する問題ではなく、両国の首脳が議論し、しかしながら明確な結論が出せない問題になっている。本稿では、米中のサイバーセキュリティ問題をめぐる動向を追っていきたい。

１．カリフォルニアでの米中首脳会談

2013年6月に米国カリフォルニア州で米中首脳会談が開かれた。その際に注目された議題の1つがサイバーセキュリティであった。バラク・オバマ（Barack Obama）米大統領は、習近平中国国家主席に対して中国から行われているサイバースパイ活動（広義のサイバー攻撃）、特に中国の政府機関による米国企業への産業スパイ活動をやめるように迫った。しかし、この会談の直前、米国政府が米国の通信会社から顧客の通信情報を大量に収集しているとの報道が出ていた[8]。オバマ大統領に対して習主席は、サイバースパイは米国のほうではないかといい返し、両国は合意することができなかった。

習近平主席は、この時点ではオバマ大統領との間で合意することはできなかったが、翌2014年2月に米国側に1つの回答を提示した。それは、中央網絡安全和信息化領導小組（中央ネットワーク安全・情報化指導小組）を組織し、習主席自ら議長（組長）に就任したことである。副議長（副組長）には李克強首相と劉雲山中央書記処筆頭書記が就いた。領導小組は中国政府の組織ではなく、中国共産党の組織だが、中国の党国体制の下では共産党が実質的な政策決定権を担っており、この領導小組がサイバーセキュリティに関連する政

策の最終決定を担うことになる[9]。

この領導小組が作られる前の 2011 年に、国家互聯網信息弁公室（国家インターネット情報弁公室）が作られており、魯煒が主任に就いていたが、この弁公室は中国政府側の組織であり、権限もはっきりしていなかった。中央網絡安全和信息化領導小組は 2014 年 2 月に最初の会合を開いた。同年 11 月には浙江省の烏鎮で第 1 回の世界インターネット大会が開かれ、世界約 100 カ国から 1000 人が集まったという[10]。

領導小組は 2015 年 1 月に 2 回目の会合を開いた。1 年に 1 回しか開かれないのでは実質的な意味はなさそうに見える。しかし、共産党側に中央網絡安全和信息化領導小組が作られ、そのトップに習主席が就いたことで、魯の弁公室も位置付けが定まり、領導小組を背景に政策を実施しやすくなった点を見過ごすべきではないとの見方もある[11]。2016 年 6 月に魯煒が主任を退き、代わりに副主任だった徐麟が主任に就任した。

しかし、2014 年はじめの段階では、こうした中国側の取り組みに米国側は満足しなかった。中央網絡安全和信息化領導小組の第 1 回会合が開かれてから 4 ヵ月後の 2014 年 5 月、米国のエリック・ホルダー（Eric Holder, Jr.）司法長官は突然記者会見を開き、中国人民解放軍の 5 人が米国企業などに対するサイバースパイ活動に携わっているとして被疑者不在のまま訴追すると発表した。5 人は中国国内にいると考えられているが、上海に拠点を置くと報道されている人民解放軍 61398 部隊の関係者とされている。この部隊は、米国のニューヨーク・タイムズ紙などに対するサイバースパイ活動に関わったとマンディアント社の報告書で名指しされていた[12]。

中国政府側は、こうした問題はまず米中政府間のサイバー・ワーキング・グループで検討されるべき問題であり、突然記者会見が開かれたことに強い不満を表明し、政府間ワーキング・グループを無期限中止にすると宣言した。米中間の政府対話は、後述する 2015 年 9 月の米中首脳会談によって高官級の対話が行われることになるまで凍結された。

その後も中国によるものと思われるサイバースパイ活動は後を絶たず、オバマ大統領は 2015 年 2 月にスタンフォード大学で民間企業の責任者たちを集めたサイバーセキュリティサミットを開催し、4 月には新たな大統領令を発した。その際、オバマ大統領は「悪意のあるサイバー活動の蔓延と深刻さは米国の国家安全保障、外交政策、経済にとって甚大な脅威となる。この脅威に対処するため、ここに私は国家非常事態を宣言する」と述べている[13]。

ところが、その直後、米国政府の人事局（OPM）から 400 万人分の個人情報がサイバースパイ活動によって盗まれた形跡があり、中国によるものである疑いが強いとの報道がなされた。その後、被害人数は 2210 万人分に達することが分かった。米国の人口の 7%に相

当し、米国政府のセキュリティクリアランス取得者 510 万人（民間人を含む）を優に上回っている。セキュリティクリアランス取得者の詳細な個人情報が含まれているとする懸念があり、米国議会の議員たちは中国を強く非難している[14]。

２．ワシントン DC での米中首脳会談

2015 年 9 月、習近平国家主席は米国を訪問し、ワシントン DC におけるオバマ米国大統領との首脳会談において「サイバー攻撃実行せず、支援せず」で合意したというニュースが流れた。両首脳の記者会見においては、オバマ大統領が発言の冒頭近くでサイバーセキュリティを取り上げたのに対し、習主席は発言の後半でわずかに言及するのみで、両者の間には温度差が見られた[15]。

これまで中国は、中国自身がサイバー攻撃の被害者であると主張し、米国との間で何らかの合意をすることをかたくなに拒否してきた。今回も中国はその姿勢を崩さず、米国側の要求をはねつけるのではないかと見られていた。首脳会談の 2 週間前、米国のメディアは、米国政府側のリークに基づき、さかんに制裁の可能性を示唆する記事を流していた[16]。しかし、中国では「制裁はない」との見方も出ていた[17]。

習主席がワシントン DC 入りする前に、中国から米国西海岸のシアトルに到着した頃、ローマ教皇がワシントン DC を訪問しており、ワシントンの関心はそちらに向いていたが、中国側は IT 業界の雄マイクロソフトと航空業界の雄ボーイングが拠点を置くシアトルで、経済に焦点を絞ったイベントを開き、米中経済が分かちがたく結びついていることをアピールした。中国でサービスが規制されているグーグルとツイッター、フェイスブックのトップは参加しなかったが（フェイスブックのマーク・ザッカーバーグ［Mark Zuckerberg］は写真撮影には応じた）、ボーイングでは中国が 300 機も発注するという「爆買い」がニュースになった。それもこれも、ローマ教皇のニュースに埋もれることなく、米中首脳会談をなんとか成功させようとする中国側の意気込みの現れであった。

ワシントン DC での米中首脳会談では、広範なテーマについてやりとりが行われたが、サイバー攻撃については、「どちらの国も知的財産を盗むサイバー攻撃を実行しないし、支援しないことで合意した」とし、「両国はサイバー犯罪について対策を話し合う年 2 回の高官級の対話メカニズムを創設する」ことになったという[18]。

先述の通り、2014 年 5 月に米国司法省が突然記者会見し、中国人民解放軍の 5 人の将校を顔写真入りで指名手配し、容疑者不在のまま起訴するという行動に出て以来、米中政府間のサイバー・ワーキング・グループは中止されたままだった。今回、それを高官級に格上げして、実質的に再開することになった。

この合意のポイントは、必ずしも中国（あるいは中国政府や人民解放軍）がこれまで米国に対するサイバー攻撃に関与してきたかどうかを認めたわけではないということである。過去に何があったかについては判断せず、「未来において」どちらの国も知的財産を盗むサイバー攻撃を実行しないし、支援しないことで合意したというところで、中国側も納得し、合意したということだろう。それによって、中国側が重視するメンツを保ち、習主席の訪米を成功させることを優先した。中国側は、首脳会談で重要なテーマにおいて決裂したとの印象・報道をどうしても避けたかったと見るべきだろう。その点では、米国側がこれまでかけてきた圧力が功を奏したとも見ることができる。

これまでも米国側の圧力はそれなりに中国を動かしてきた。実際、2015 年 9 月の習主席の訪米前に、中国は国内のサイバー犯罪者を大量に検挙するとともに[19]、孟建柱・中国共産党中央政法委員会書記（サイバー問題特使）がワシントン DC に先乗りして米国政府関係者との事前協議を行っている。

米中首脳会談は決裂を回避し、習主席は訪米を一応成功させることができた。しかし、いったん合意してしまった以上、その履行が求められることになる。中国側が米国からのサイバー攻撃に文句を付けられるようにもなるが、中国側が自国から米国に向けたサイバー攻撃、サイバースパイ行為を止められるかが最大の関心事になった。

３．中国におけるサイバー攻撃の担い手

2015 年 9 月の米中首脳会談で中国がサイバー攻撃をしないと合意した直後、米国のインテリジェンス・コミュニティを束ねるジェームズ・クラッパー（James Clapper）国家情報長官（DNI）は、「合意が守られる見通しはない」と議会上院の軍事委員会の公聴会で証言していた[20]。実際、首脳会談後も中国から米国へのサイバー攻撃は止まっていないという報道も出た[21]。

先述の通り、2013 年 2 月の米国マンディアント社の報告書で人民解放軍の 61398 部隊が名指しされ、2013 年 6 月のカリフォルニアでの米中首脳会談ではバラク・オバマ米大統領が中国の習近平国家主席に直接懸念をぶつけた。2014 年 5 月には米国司法省が 5 人の中国人民解放軍の軍人たちを指名手配し、被疑者不在のまま起訴すると発表した。その後も、米国の官と民による中国名指しが続き、2015 年 9 月の米中首脳会談では経済制裁が行われるのではないかという見通しも出ていた。

こうした米国の戦術は「名指しと恥さらし（Name and Shame）」といわれている。メンツを重んじる中国社会ではこれは十分に効き目があると見られていた。米中首脳会談のような注目される場面において不正な行いをしていると面と向かっていわれれば、さすがに

中国も対応をとるのではないかというのが米国側の希望的観測だった。

首脳会談で中国側は、これまでの原則を繰り返し、口頭では合意したものの、文書に残すことは拒否した。それでも、米国側にとっては、両首脳が並んで記者会見し、言質を取ったという点では一応の勝利だった。

しかし、中国国内ではこうした合意は報道されず、習主席の米国訪問が成功に終わったという論調の報道ばかりになった。無論、中国のインターネット利用者の多くも国外の報道を目にしており、中国政府の一方的な報道が必ずしもバランスのとれたものでないことは気づいている。それでも、多くの人は習主席のメンツが失われたとは思っていない。

こうした事態の推移を見て、中国側の戦術は「話と盗み（Talk and Take）」に他ならないという怒りの声が米国から出た[22]。対話を続ける振りをしながら、その間にどんどん米国の知的財産を奪っているという声である。

そもそも誰が中国でサイバー攻撃を行っているのか。

第一に、不満を持つ若者たちである。中国の経済成長は鈍化しつつあり、大学を卒業しても仕事がない若者たちが多くなっている。経済が豊かになるにつれ、かつてのように、どんな仕事でも良いというわけにはいかなくなり、見栄えと実入りの良い仕事を競うようになっている。そうした仕事に就けない若者たちは、地下の穴蔵のような地下室で共同生活を送り、「アリ族」や「ネズミ族」とも呼ばれ、不満のはけ口をサイバー攻撃に見いだしている[23]。

第二に、経済的な利得につながる情報を盗み出そうとしている人たちである。こうした人たちは国内外問わず、金儲けになりそうな情報は何でも盗もうとしている。中国企業が中国企業に対してサイバー攻撃を仕掛けることも無数にある。産業スパイは日常茶飯事ともいって良い。

第三に、よく名指しされる人民解放軍である。彼らも経済的利得につながるサイバー攻撃を行うことがあり、米国が最も非難しているのはそうした攻撃である。しかし、軍事的な切り札としてのサイバー攻撃はまだ行っておらず、温存しているはずである。平時に使ってしまっては意味がない。むしろ、戦時に備えた偵察行動が行われている。

第四に、政治的なスパイである。中国国内では全てが権力闘争といっても良い状態である。そうした国内事情を国外にも投影し、中国の政治アクターは、米国や日本の国内の権力闘争の実態を知りたがる。米国や日本でそうした権力闘争が全くないとはいわないが、中国のような苛烈な政治闘争はほとんど見られないため、ほとんど存在しない情報を必死に中国のスパイたちは探している。

こうした多様な攻撃者たちが存在するとしたら、中国共産党が抑えられるのはどこまで

か。米中首脳会談の際、習主席は「13 億人全ての行動は保証できない」とオバマ大統領に釘を刺したという[24]。つまり、習主席が全てのサイバー攻撃者を止められるわけではないという意味である。中国では検閲が行われているから簡単に摘発できるといわれるが、6 億人ものインターネット利用者がいると簡単ではない。インターネットについては、中国政府は人民一人一人の統制からインターネット事業者を通じた統制へと切り替え始めている。事業者の顧客が何か悪いことをすれば営業許可を取り消すと圧力をかけ、間接的な統制をしようとしている（中国ではコンテンツ事業者にも営業許可が必要である）。事業者は、当局を怒らせず、顧客の不満も最小化できる線（中国では「底線」と呼ばれる）がどこにあるのか探している状態である[25]。

常識的に考えれば、非政府アクターとしての若者たちと経済スパイたちを全て止めるのは難しいとしても、人民解放軍と政治スパイは共産党の力で止められると考えられるだろう。しかし、いずれのサイバー攻撃も止まらないと米中会談直後の米国側は見ていた。ところが、2016 年 6 月には中国によるサイバー攻撃が米国に対しては減少し、ロシアやインドで増加したという報道が出てきた[26]。

４．安定化する米中と不安定化する米露

2016 年 9 月 3 日、米中は、中国の杭州で開かれた G20 の機会を捉え、首脳会談を行った。この席ではサイバーセキュリティはもはや最重要課題ではなくなっていた。米国側の発表文書を見ると、「グローバルないし地域的な課題への対処」として 16 項目が挙げられ、「二国間関係の強化」として 6 項目が挙げられた。サイバーセキュリティはこのうち、「二国間関係の強化」の第 4 番目になっている。サイバーセキュリティの項目の冒頭では、以下のように述べられている。

> 両国は 2015 年 9 月のサイバーに関する約束を十分に実施する意図を再確認する。それには悪意のあるサイバー活動やハッキングと戦い、商業的な利得のためにサイバーを使った知的財産権の窃盗を行ったり、知った上で支援したりしないことを含む[27]。

この米中首脳会談の後、中国の研究者に対してヒアリングを行ったところ[28]、米国政府から頻繁に高官が北京に来るなど、「我々は米国ときわめて良好な意見交換ができている」との発言が聞かれた。

ところが、続けて出てきた発言は、「なぜロシアはウクライナや米国民主党全国委員会な

どに対してサイバー攻撃を行うのか。なぜロシアは国連 GGE 報告書に従わないのか」というものだった。国連 GGE 報告書とは、国連総会第 1 委員会で続けられている政府専門家会合（GGE）での報告書である。2016 年 8 月から第 5 期の会合が行われているが[29]、2015 年に第 4 期の報告書が発表されている[30]。ロシアは GGE での議論を主導してきた国であり、サイバースペースの悪用に少なくとも名目上は反対してきた。それにもかかわらず、各種のサイバー攻撃を展開していることに中国の研究者が疑念を表したことになる。

米国のサイバーセキュリティ議論では長らく中国が最大の悪玉だったが、2016 年の米国大統領選挙をきっかけにその座はロシアに移った感がある[31]。そもそも今回の大統領選挙はひどい暴露合戦だった[32]。米国の大統領選挙では、予備選の段階からさまざまな暴露が行われるのが常であり、スキャンダルを暴露された候補者は次々と選挙戦から脱落していくのが通例であった。ところが、ヒラリー・クリントン（Hilary Clinton）民主党候補も、ドナルド・トランプ（Donald Trump）共和党候補も、数々の暴露をくぐり抜けて各党の指名を勝ち得た。

クリントン候補の場合、まず問題になったのが国務長官時代に私用の電子メールアカウントを公用に用いていたことであった。国務長官の電子メールには機密情報も送られてくる。国務省の専用の電子メールアカウントを用いていれば問題にならなかっただろう。しかし、おそらくは機密情報保護のために使いにくいシステムであったため、国務長官は省の了解を得た上で私用アカウントを使っていた。

ところが、彼女の在任中の 2012 年にリビアのベンガジで米国大使他 4 人が殺害されるという事件が起きてしまう。遺族たちは、当時のクリントン長官が私用アカウントを使っていたと知ると、そこから機密が漏洩しており、事件につながったのではないかと疑うようになり、クリントン候補は強い批判を浴びることになった。連邦捜査局（FBI）がクリントン候補に事情聴取を行い、公務に関わる電子メールが公開されることになった。その結果、いくつか問題のある機密情報の取り扱いはあったものの、訴追は行わないと FBI と司法省は判断した。

クリントンは電子メール問題を逃げ切ったかと思われたが、2016 年 6 月になって、今度はサイバー攻撃によって奪われたと見られる民主党全国委員会（DNC）の電子メールが暴露されてしまう。暴露情報サイトとして知られるウィキリークスや、Guccifer 2.0 と呼ばれる人物が解説したサイトなどで公開された。Guccifer はもともとルーマニアの悪玉ハッカーのハンドルネームで、彼はすでに有罪で収監されている。Guccifer 2.0 はもとの Guccifer とは関係ない。米国のインテリジェンス（情報・諜報）機関は、ロシア軍参謀本部情報総局（GRU）が関係していると見ている。

DNC の電子メールによって民主党全国委員会の内情が暴露され、もうひとりの民主党の有力候補だったバーニー・サンダース（Bernie Sanders）よりもクリントンがひいきされていることが分かり、委員長は辞任に追い込まれた。

他方、トランプのほうでも、候補になる以前からの数々の問題発言が取りざたされた。特に、セクシャルハラスメントに当たる音声テープが暴露されたり、納税を回避していることを示唆するような文書が暴露されたりといったことが起きた。しかし、トランプは過激な発言が持ち味でもあり、セクハラや納税問題は一時的なダメージにしかならなかった。

こうした混乱に拍車をかけたのが、出所不明の偽ニュースである。「ローマ教皇がトランプを支持した」、「ワシントン DC のピザ店が小児性愛と児童売春の拠点になっており、クリントンがそれに関わっている」といったデマがソーシャルメディアで拡散されるようになった。

2016 年 12 月に退任間近のオバマ大統領は、大統領選挙に介入するためにサイバー攻撃を行ったとして、ロシアに対して政治的な制裁を発動し、ロシアの外交官 35 人を追放し、ロシア政府が米国内で使っていた拠点 2 つを閉鎖した。

ロシアは、これまでロシアの体制批判を繰り返してきたクリントン候補への意趣返しとして暴露や偽ニュースを出してきたのだろう。トランプの当選まで本気で狙っていたのかどうかは分からない。仮にクリントンが勝つにしても、その勝利に米国民が疑念を持ち、米国の民主政治そのものの根幹を揺るがすことができればと考えていたのではないだろうか。トランプが当選した現在、逆にトランプ政権に対するデモが行われるようになっている。こうした現状は、ロシアにとっては好ましい展開であろう。

トランプは当選してからも長く記者会見を行わなかったが、2017 年 1 月 11 日、ようやく記者会見を行った。その直前、インターネットメディアのひとつ、バズフィードがトランプにまつわる 35 ページの暴露文書をウェブ上で公開した[33]。文書は英国のインテリジェンス機関の元職員が書いたもので、長らく密かにワシントン DC で出回っていたものである。そこにはトランプ大統領に関する問題ある情報をロシア政府が握っていると示唆されているが、これも真偽不明のままである。これに怒ったトランプは、バズフィードやそれを報じた CNN を記者会見で非難し、質問を許さなかった。

現代の情報通信技術（IT）は、強力な暴露ツールである。以前は隠されていたような情報が簡単にインターネット上で共有されるようになっている。米国国務省の公電を暴露したウィキリークスや、米国国家安全保障局（NSA）の機密文書を暴露したエドワード・スノーデン（Edward Snowden）は、IT なくしては登場し得なかっただろう[34]。IT は正確なコピーを世界中に瞬時に届けることができる。虚実入り混じる暴露が常態化していくことに

なるだろう。

民主主義体制においては自由な言論が基盤となっている。その点についてクリントンはロシアを批判してきた。ロシアから見れば、そうした批判自体が情報による攻撃に他ならない。それに対する反撃として米国の自由なメディア基盤を悪用しながら大統領選挙に介入を行った。

ロシアによる大統領選挙介入があったことを認めることは、トランプ大統領にとっては自分の正当性に疑念を投げかけることになる。ロシアにとっては、トランプが当選してもクリントンが当選しても、米国の民主主義体制に疑問を持つ人が増えれば情報テロに成功したことになる。

こうしたサイバーセキュリティにおけるロシアの悪玉化は、必ずしも今に始まったことではないが、2016 年の米国大統領選挙で一気に注目されることになり、中国と位置が入れ替わったといって良いだろう。中国がサイバー攻撃を米国に対し控え、ロシアが攻勢をかけている背景には、米中が経済によって深く結びついているのに対し、米露はすでに経済制裁が数年にわたって続いており、もともと米中ほど強い経済関係がなかったことも影響しているだろう。

おわりに

サイバー紛争やサイバー戦争の可能性をめぐる議論は、それらの「定義」によることは多くの人が理解している。英国キングス・カレッジのトーマス・リッド（Thomas Rid）は、破壊的なサイバー戦争は来ないと論じた[35]。ブランドン・ヴァレリアーノ（Brandon Valeriano）とライアン・マネス（Ryan Maness）は実証的に見てもそうした事例がほとんどないことを指摘している[36]。

サイバー領域だけで完結して行われる「サイバー戦争」はすでに起きているが、人命の損失や物理的な被害をもたらすような深刻なものになっていない。最初の「世界ウェブ大戦」といわれる 2007 年のエストニアに対する DDoS（Distributed Denial of Services）攻撃に始まり、2009 年の米韓に対する同時 DDoS 攻撃[37]、2010 年の尖閣諸島をめぐる日本に対するサイバー攻撃、2014 年のソニー・ピクチャーズエンタテインメントに対する攻撃など枚挙に暇がない。さらにはサイバー・エスピオナージの範疇に入るサイバー攻撃は無数といって良い規模で行われている。米国のセキュリティ会社であるファイアアイはこれまでにも APT1[38]、APT28[39]、APT30[40]などいくつかのサイバー・エスピオナージに従事するグループについて明らかにしているし、他の会社はドラゴン・フライ[41]、パターパンダ[42]、ダークホテル[43]など様々なサイバー・エスピオナージ活動を明らかにしており、それらを「サイバー

戦争」と呼ぶならば、すでにそれは起きている。

そうだとすれば、それらを超える狭義の「サイバー戦争」は起きるのだろうか。これらの活動を超えるサイバー攻撃があるとすれば、それらは必然的に物理的な被害を伴うことになる。サイバー攻撃が物理的な攻撃と組み合わせられるとき、それは非常に高い蓋然性でこれから起きるだろう。いいかえるなら、今後行われる戦争においてサイバー攻撃の要素は必須になる。それが、敵国・敵勢力の軍事システムに対する攻撃ならば、それは国際法の武力紛争法の範囲に収まる。しかし、民間システムにまでそれが及ぶとすれば、国際法で適切に処理できない領域にならざるを得ない。それをどう防止・抑止・抑制するかが現在の課題である。

米国が首脳レベルで中国を非難し、対応を求めることで、何らかの意味ある合意が形成されれば、それは国際的なスタンダードになり得る。しかし、サイバーセキュリティにおける米国の関心は、2017 年初めの段階ではロシアに向けられるようになっており、中国の影はやや薄くなった感がある。それでも、この状態が永続的なものになるとは考えにくい。サイバーセキュリティは現実世界の地政学的な関係を反映したものであり、米中関係がトランプ政権の下で悪化することになれば、再び懸念材料になるだろう。

－注－

1　本稿は以下の既存の原稿を加筆修正し、再構成したものである。土屋大洋「中国のサイバーセキュリティをめぐる霧」日本国際問題研究所編『US-China Relations Report』<https://www2.jiia.or.jp/RESR/column_page.php?id=241>、Vol. 1、(2015 年)。土屋大洋「意外だが、よく分かる米中のサイバー合意」『Newsweek 日本版』<http://www.newsweekjapan.jp/tsuchiya/2015/09/post-4.php>、(2015 年)。土屋大洋「効き目がなかった米国の対中サイバー交渉戦術」『Newsweek 日本版』<http://www.newsweekjapan.jp/tsuchiya/2015/11/post-9.php>、(2015 年)。土屋大洋「サイバーセキュリティ政策をめぐる中国政府の内側」『Newsweek 日本版』<http://www.newsweekjapan.jp/tsuchiya/2016/01/post-11.php>、(2016 年)。

2　Michael N. Schmitt, ed., *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013), Rule 30.

3　Thomas Rid and Ben Buchanan, “Attributing Cyber Attacks,” *Journal of Strategic Studies*, 38:1-2, (2015), pp. 4-37, DOI: 10.1080/01402390.2014.977382.

4　Dylan Tweney「飛行機を座席からハッキング可能、FBI が指摘」『日本経済新聞』<http://www.nikkei.com/article/DGXMZO87033730Q5A520C1000000/>、2015 年 5 月 21 日。Kim Zetter, “Hacker's Tweet Reignites Ugly Battle over Security Holes,” *Wired* <http://www.wired.com/2015/04/twitter-plane-chris-roberts-security-reasearch-cold-war/>, April 21, 2015. Danny Yadron「ハッカー、「ジープ」を遠隔操作でハイジャック」*Wall Street Jounal* <http://jp.wsj.com/articles/SB10777827119304873821304581123650751271000>、2015 年 7 月 22 日。実験の動画は以下で公開されている。Andy Greenberg, “Hackers Remotely Kill a Jeep on the Highway—With Me in It,” *Wired* <http://video.wired.com/watch/wired-s-top-five-security-stories-of-2015>, July 21, 2015.

[5] Kim Zetter, *Countdown to Zero Day: STUXNET and the Launch of the World's First Digital Weapon* (New York: Crown Publishers, 2014).

[6] Bundesamt für Sicherheit in der Informationstechnik, "Die Lage der IT-Sicherheit in Deutschland 2014," *Bundesamt für Sicherheit in der Informationstechnik* <http://www.wired.com/wp-content/uploads/2015/01/Lagebericht2014.pdf>, 2014, p. 31. 原文はドイツ語だが、該当箇所は以下のブログで英訳されている。Robert M. Lee, "ICS Cyber-Attack on German Steelworks Facility and Lessons Learned," *Dragos Security* <https://dragossecurity.com/blog/9-ics-cyber-attack-on-german-steelworks-facility-and-lessons-learned> December 18, 2014. その他に関連する報道としては以下を参照。BBC, "Hack Attack Causes 'Massive Damage' at Steel Works," *BBC* <http://www.bbc.com/news/technology-30575104>, December 22, 2014; Kim Zetter, "A Cyberattack Has Caused Confirmed Physical Damage of the Second Time Ever," *Wired* <http://www.wired.com/2015/01/german-steel-mill-hack-destruction/> January 8, 2015; Eduard Kovacs, "Cyberattack on German Steel Plant Caused Significant Damage: Report," *Security Week* <http://www.securityweek.com/cyberattack-german-steel-plant-causes-significant-damage-report> December 18, 2014; Loek Essers, "Cyberattack on German Steel Factory Causes 'Massive Damage,' " *IT World* <http://www.itworld.com/article/2861675/cyberattack-on-german-steel-factory-causes-massive-damage.html> December 19, 2014.

[7] 例えば、以下を参照。James Titcomb, "Ukrainian Blackout Blamed on Cyber-attack," *Telegraph* <http://www.telegraph.co.uk/technology/news/12082758/Ukrainian-blackout-blamed-on-cyber-attack-in-world-first.html>, January 5, 2016.

[8] 後にこの報道は、米国国家安全保障局（NSA）の契約職員だったエドワード・スノーデンが大量に持ち出した機密情報に基づく報道であることが明るみになり、その後も次々と NSA の秘密活動が暴露されることになった。2013 年の後半は、スノーデン情報に基づく報道が断続的に続いた。

[9] 領導小組はさまざまな政策分野で設けられている。例えば、外交・安全保障を担っているのは中央外事工作領導小組（中央国家安全保障領導小組）である（両組織は同じメンバーで構成されていると思われる）。

[10] 「世界インターネット大会、中国・浙江省で開幕」『日本経済新聞』< http://www.nikkei.com/article/DGXLASGM19H2R_Z11C14A1FF1000/>、2014 年 11 月 20 日。

[11] 2015 年 9 月、聞き取り調査による。聞き取り先の都合により匿名。

[12] Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," *Mandiant* <http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf>, February 18, 2013.マンディアントの報告書が注目されたのは、2012 年 10 月に中国の温家宝首相に関する不正蓄財報道以降、サイバー攻撃を受けていたとされるニューヨーク・タイムズ紙の報道の効果も大きい。David Barboza, "Billions in Hidden Riches for Family of Chinese Leader," *New York Times* <http://www.nytimes.com/2012/10/26/business/global/family-of-wen-jiabao-holds-a-hidden-fortune-in-china.html>, October 25, 2012.

[13] The White House, Office of the Press Secretary, "Executive Order – 'Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities,'" *White House* <https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m>, April 01, 2015.

[14] 例えば、以下を参照。Senator Ben Sasse, "Senator Sasse: The OPM Hack May Have Given China a Spy Recruiting Database," *Wired* <http://www.wired.com/2015/07/senator-sasse-washington-still-isnt-taking-opm-breach-seriously/>, July 9, 2015.

[15] The White House, Office of the Press Secretary, "For Immediate Release: Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference," *White House* <https://www.whitehouse.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint>, September 25, 2015.

[16] 例えば、以下を参照。Andrew Blake, "Xi Calls for Cyber Dialogue between China, U.S. as Sanctions Talk Looms," *Washington Times* <http://www.washingtontimes.com/news/2015/sep/23/xi-calls-cyber-dialogue-between-china-and-us-sanct/>, September 23, 2015. 「米政府、サイバー攻撃での対中制裁を準備　習主席の訪米控え」*CNN* <http://www.cnn.co.jp/usa/35069724.html>、2015 年 9 月 1 日。

[17] 2015 年 9 月、聞き取り調査による。聞き取り先の都合により匿名。
[18] 「米中首脳会談　サイバー対策で対話、合意」『毎日新聞』<http://mainichi.jp/articles/20150926/ddn/001/030/005000c>、2015 年 9 月 26 日。
[19] 「中国、サイバー犯罪取り締まりで 1 万 5000 人を逮捕」*CNN* <http://www.cnn.co.jp/tech/35069127.html>、2015 年 8 月 19 日。
[20] Andrea Shalal, “Top U.S. Spy Says Skeptical about U.S.-China Cyber Agreement,” *Reuters* <http://www.reuters.com/article/us-usa-cybersecurity-idUSKCN0RT1Q820150930>, September 30, 2015.
[21] 「米企業 7 社に中国のサイバー攻撃、首脳会談後＝クラウドストライク」『ロイター通信』<http://jp.reuters.com/article/usa-china-cybersecurity-idJPKCN0SD0GU20151019>、2015 年 10 月 19 日。
[22] “The Obama-Xi Cyber Mirage: A Digital Arms Deal that is Full of Promises but No Enforcement,” *Wall Street Journal* <http://www.wsj.com/articles/the-obama-xi-cyber-mirage-1443387248>, September 27, 2015.
[23] 石平『中国ネット革命』（海竜社、2011 年）。
[24] 「米中首脳会談　米大統領『行動が重要』　サイバー問題、中国にクギ」『毎日新聞』<http://mainichi.jp/articles/20150927/ddm/001/030/152000c>、2015 年 9 月 27 日。
[25] インターネット規制における「底線」については以下を参照。佐藤千歳『インターネットと中国共産党―「人民網」体験記―』（講談社文庫、2009 年）。
[26] 「中国のサイバー攻撃による産業スパイ行為、米国で減少＝専門家」『ロイター通信』<http://jp.reuters.com/article/cyber-spying-china-idJPKCN0Z707T>、2016 年 6 月 21 日。
[27] White House, “U.S. Fact Sheet for President Obama’s Bilateral Meeting with President Xi Jinping,” *White House* <https://obamawhitehouse.archives.gov/the-press-office/2016/09/03/us-fact-sheet-president-obamas-bilateral-meeting-president-xi-jinping>, September 03, 2016.
[28] 2016 年 9 月、聞き取り調査による。聞き取り先の都合により匿名。
[29] 土屋大洋、齋藤敦「政府はサイバー空間を守れるか」『外交』第 40 号（2016 年 11 月）49～60 頁。
[30] United Nations General Assembly, “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General,” *United Nations* <http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174>, July 22, 2015.
[31] 以下の記述は次の原稿に基づく。土屋大洋「虚実入り交じる暴露の時代が到来」*WEBRONZA* <http://webronza.asahi.com/politics/articles/2017020800005.html>、2017 年 2 月 14 日。
[32] 土屋大洋『暴露の世紀　国家を揺るがすサイバーテロリズム』（角川新書、2016 年）。
[33] Ken Bensinger, Miriam Elder, and Mark Schoofs, “These Reports Allege Trump Has Deep Ties to Russia,” *BuzzFeed* <https://www.buzzfeed.com/kenbensinger/these-reports-allege-trump-has-deep-ties-to-russia?utm_term=.nvK09mbLZ#.ek3LglaN2>, January 11, 2017.
[34] 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）。
[35] Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst and Company, 2013).
[36] Brandon Valeriano, and Ryan Maness, “The Fog of Cyberwar: Why the Threat Doesn’t Live Up to the Hype,” *Foreign Affairs*, November 21, 2012.
[37] Motohiro Tsuchiya, “Cybersecurity in East Asia: Japan and the 2009 Attacks on South Korea and the United States,” Kim Andreasson, ed., *Cybersecurity: Public Sector Threats and Responses* (Boca Raton, FL: CRC Press, 2012), pp. 55-76.
[38] Mandiant, “APT1: Exposing One of China’s Cyber Espionage Units,” *Mandiant* <http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf>, February 18, 2013, accessed on May 22, 2014. マンディアントはファイアアイと合併した。
[39] FireEye, “APT28 - A Window into Russia’s Cyber Espionage Operations?” *FireEye* <https://www2.fireeye.com/apt28.html>, accessed on July 13, 2015.
[40] FireEye, “APT30: The Mechanics Behind a Decade Long Cyber Espionage Operation,” *FireEye* <https://www2.fireeye.com/WEB-2015RPTAPT30.html>, accessed on July 13, 2015.
[41] Symantec, “Emerging Threat: Dragonfly / Energetic Bear – APT Group,” *Symantec* <http://www.symantec.com/connect/blogs/emerging-threat-dragonfly-energetic-bear-apt-group>, accessed on July 13, 2015.

[42] CrowdStrike Global Intelligence Team, “CrowdStrike Intelligence Report: Putter Panda,” *CrowdStrike* <http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf>, June 2014, accessed on June 18, 2014.

[43] Kaspersky Lab’s Global Research & Analysis Team, “The Darkhotel APT: A Story of Unusual Hospitality,” *Kaspersky Lab* <https://securelist.com/blog/research/66779/the-darkhotel-apt/>, accessed on July 13, 2015.