

国際政治とサイバー攻撃に関する2018年の動き

土屋 大洋 ●慶應義塾大学大学院 政策・メディア研究科 教授

政府によるサイバー攻撃疑惑などサイバースペースの軍事的色彩強まる。新防衛大綱もサイバー反撃能力強化を盛り込む。一方、国際規範の整備を呼びかける動きも活発に。

■軍事的な措置をとる米国

ロシア政府がサイバー攻撃やフェイクニュースを通じて2016年米国大統領選挙に介入したのではないかとする疑惑は依然として2017年、そして2018年にも米国政治の焦点の1つであった。ドナルド・トランプ候補の選挙対策本部長であったポール・マナフォートや個人弁護士だったマイケル・コーエンが偽証を認めるなど、ロバート・マラー特別検察官の捜査は続いている。

しかし、トランプ政権はサイバーセキュリティ問題を避けることもなく、むしろ積極的な取り組みを続けている。2017年8月、トランプ大統領はサイバー軍を最上位の統合軍に昇格させると発表していたが、2018年5月、それを実施した。

米軍の軍種には、陸軍、海軍、空軍、海兵隊があるが、実際の戦闘にあたっては、それぞれから必要な部隊を集め、統合軍として編成される。従来の統合軍は地域別に6つ、機能別に3つあったが、サイバー軍 (USCYBERCOM) は機能別統合軍の1つである戦略軍 (USSTRATCOM) の下に位置づけられていた。そこからサイバー軍は昇格し、10番目の統合軍となった。同時に、三代目のサイバー軍司令官として日系のポール・ナカソネが任命された。

こうした再編は、米軍の活動においてサイバーセキュリティがいつそう重要になってきていることを示している。実際、イスラム国や北朝鮮に対してサイバー攻撃を実施したことを政権幹部が公言するようになった。

2018年9月には、国防総省がサイバーセキュリティ戦略を発表した。しかし、軍事作戦に関わるものなので、一般向けにはサマリーだけが公開された。その中で注目されるのは、「前方で防衛する (defend forward)」という言葉が入ったことである。米軍は米国本土における戦闘を想定せず、欧州やアジアに米軍基地を確保するという前方展開を旨としている。サイバーセキュリティにおける前方防衛は、米国本土においてサイバー攻撃が行われる前に、攻撃者が属する外国において攻撃を食い止めることを意味する。これは平時から仮想敵のネットワークを監視しておかなければできない。サイバーセキュリティにおいては平時と戦時の区別がつかなくなっており、大きなグレーゾーンが広がっていることを示している。

■経済目的の活動を続ける北朝鮮

2017年中に北朝鮮がミサイル発射実験を繰り返していた間は、米軍によるサイバー攻撃が北

朝鮮に対して行われた。当時、北朝鮮のインターネット接続は中国との回線に依存していたが、米軍がこの回線に分散型サービス拒否（DDoS）攻撃をかけたことで、北朝鮮はインターネットに接続ができなくなった。北朝鮮は慌ててロシアとの回線を開設して対応した。

2018年6月にシンガポールで米朝首脳会談が開かれると、北朝鮮問題は新たな段階に入ったと見られた。しかし、北朝鮮の非核化はなかなか進まず、1950年以来の朝鮮戦争の終結も公式には宣言されていない。

政治的・軍事的な目的のサイバー攻撃とは別に、北朝鮮は外貨獲得のためのサイバー攻撃・サイバー犯罪にも積極的であり、そうした活動は依然として続いていると見られている。特に、ビットコインなどの仮想通貨をめぐるサイバー犯罪では活発に動いている。

■米中貿易摩擦に揺れる中国

2015年9月にバラク・オバマ大統領との間で行われた米中首脳会談において中国の習近平国家主席は、経済目的での政府機関によるサイバー攻撃を行わないことで合意した。2017年にトランプ政権が成立し、トランプ大統領との首脳会談においても中国はこの合意を遵守することを確認した。これによって一時は沈静化したと見られた中国からの米国に対するサイバー攻撃だったが、結局は高度化した攻撃手法で続けられていることが分かっている。また、経済目的ではないサイバー攻撃やサイバーエスピオナージ（スパイ活動）には両国とも積極的である。

そして、米国のトランプ大統領が対中貿易赤字に業を煮やし、対中経済制裁を実施に移すと、中国のサイバー攻撃による米国の知的財産権の窃取に対する非難も繰り返されるようになった。

中国側も対抗的措置をとったり、譲歩案を提示

したりしているが、中国経済の失速は明らかになりつつある。2018年11月初旬に中国の烏鎮で開かれた世界インターネット大会では、前年のように米国の大手IT企業のトップが登壇することではなく、中国政府幹部からは「集体治理」、つまり集団的ガバナンスを求める声が聞かれた。かつては8億人という世界最大のインターネット利用者数を抱える中国がインターネットガバナンスにおいても主導権を握るという論調が聞かれたが、米国その他の国と共同でガバナンスを実施したいという方向へ転換していることがうかがえた。

中国の民間企業も、人工知能（AI）への積極投資を進めてきたが、革新的なサービスにつながっていない。スマートフォン（スマホ）を使ったモバイル決済は中国経済に深く浸透しつつあるが、たとえば、2017年には画期的とされた大都市でのシェアサイクル（自転車共有）サービスは、2018年には失速が明らかとなり、使えなくなった大量の自転車が放置される事態になっている。

そんななか、2018年10月に、米国メディアのブルームバーグは、中国人民解放軍が米国企業のサーバー基盤に極小チップを埋め込み、データを窃取していたと報じた。当初の設計図にはないチップが中国の工場で作られて出荷され、アップルやアマゾンウェブサービス（AWS）などのサーバーとして使われた。AWSのクラウドサービスの利用者には米国中央情報局（CIA）、米国海軍、米国国防総省などが含まれており、そうした利用者のデータが盗み読まれていたのではないかと疑われている。当事者のアップルやAWSは否定的な声明を発表しており、後追い報道をするメディアがないため、報道の正確性を疑う声もあるが、ブルームバーグは、米国政府や企業との関係者17人から証言を得ているとしている。

この事案の当否はともかく、製造段階や配送段階で不正な部品やプログラムを仕込むサプライ

チェーン攻撃の可能性はかねてから指摘されており、利用者はそうしたリスクを念頭に置きながら製品やサービスを使わざるを得なくなった。

2018年12月、米国政府は、中国政府が関わるハッカー集団（APT10）が主導したサイバー攻撃で、日本を含む12か国が被害を受けたと発表した。中国政府は強く反発したが、日本、オーストラリア、ニュージーランドなど各国政府が米国政府と歩調を合わせ、中国非難に加わった。

■挑発を続けるロシア

ロシアは2018年7月、モスクワの世界貿易センターにおいて国際サイバーセキュリティ総会を開催した。ユージン・カスベルスキーなどロシアのサイバーセキュリティ業界を代表する人物が登壇したほか、ウラジミール・プーチン大統領も登壇した。

プーチン大統領は演説の中で「デジタルフリーダム」という言葉を使った。「効率的なデジタル展開は、進展を妨げる障壁を撤廃することに関する、ビジネス、公的組織、市民のためのデジタルフリーダムにだけ基づくということを指摘したい。しかし、それにもかかわらず、我々はみな、デジタル領域の挑戦とともに、責任と潜在的なリスクや脅威についても理解する必要がある」と言う。つまり、制約付きのデジタルフリーダムであり、絶対的なデジタルフリーダムの追求を目指すわけではない。

演説の後半でプーチン大統領はこうも言った。「すでに述べたように、我々の荒れ狂うデジタル時代は、自由に依存しており、それは経験とアイデアを交換し、コミュニケーションをする自由を含んでいる。」ロシアは2016年の米国大統領選挙に介入したとされる一方で、フェイクニュースの発信源としても知られている。国内では反政府、反プーチンを鮮明にするブロガーたちを抑圧し

ているともいわれている。それにもかかわらず、「デジタルフリーダム」という言葉をあえて使った点が興味深い。

そして、プーチン大統領は国際協力の重要性を力説した。サイバー犯罪に関する情報を国際的に交換するための担当機関も選定するという。

■サイバースペースの国際規範を求める動き

プーチン大統領の国際協力の重要性への言及を裏打ちするように、ロシア外務省は再び国際連合総会第一委員会の下での政府専門家会合（GGE）再開を公式に呼びかけた。5回目となるGGEの会合は、2017年夏、合意文書を作ることができずに解散している。6回目となるGGEは2019年から3年かけてじっくり議論する見通しとなっている。

しかし、2017年のGGEの不合意は、他の組織の活動を活発にした。その1つが、2017年に設立されたサイバースペースの安定性に関するグローバル委員会（GCSC）である。GCSCには、26人の委員が各国から任命されている。事務局はオランダのハーグ戦略研究センター（HCSS）および米国のイースト・ウエスト・インスティテュート（EWI）が担っている。GCSCはサイバースペースの安定性に資する国際規範の作成に力を入れており、最終案を2019年に発表する見込みである。

2018年7月、国連のアントニオ・グテーレス事務総長はデジタル協力についてのハイレベルパネルを組織した。共同議長は米国のビル&メリンダ・ゲイツ財団のメリンダ・ゲイツと、中国のアリババグループのジャック・マーである。そして世界各国から18人のメンバーが選ばれた。

2018年11月には、パリで開かれたインターネット・ガバナンス・フォーラム（IGF）の席でフランスのエマニュエル・マクロン大統領が「サ

イバー空間の信頼性と安全性のためのパリ・コール」を発表した。そこでは、悪意あるオンライン活動の予防、強靱性の向上、選挙プロセスへの干渉を防ぐための協力、サイバー傭兵や非国家主体の攻撃に対する対抗措置の実施、適切な国際規範強化への協力などが謳われた。

これらの国際規範に向けた動きは、国際条約に直結するわけではない。しかし、サイバースペースが完全な無法地帯でもないことを示すことには意義がある。そもそも、サイバー能力で先行する米国に手枷足枷を付けるため、そして、自国における各種の検閲・規制を正当化するために、中国やロシアなど権威主義体制をとる国々はサイバースペースの条約を求めている。しかし、米国や日本は、情報の自由な流通や表現の自由の観点から、既存の国際法をサイバースペースに適用すれば十分という立場をとっている。従来、欧州は日米と同様の立場をとっていたが、2018年にEU一般データ保護規則（GDPR）が実施されたように、個人データの保護のための規制を強めている。

■日本の防衛大綱

サイバースペースをめぐる安全保障が重要性を増すなか、2018年1月に日本の安倍晋三首相は、新しい防衛計画の大綱（防衛大綱）を年末までに定める方針を示した。前回の防衛大綱は2013年に定められている。通常、防衛大綱は10年をめぐりに改定されることになっているが、今回は急速に変化する安全保障情勢に対応するために改定されることになった。

今回の改定のポイントは、自由民主党が5月に発表した提言にあるとおり、宇宙・サイバースペースでの能力強化を念頭に置いたクロスドメイ

ン攻撃にあるとされた。政権与党（自由民主党および公明党）において検討が進むとともに、政府は8月に安全保障と防衛力に関する懇談会を設置し、有識者9名を任命して同時並行で検討が進められた。

12月に発表された新しい防衛大綱では、自衛隊によるサイバー反撃能力の強化などが盛り込まれ、既存のサイバー防衛隊の人員増を含め施策が見直されることになった。

■軍事的な色彩を強めるサイバースペース

これまで述べてきたような国際政治における動きを総括すれば、サイバースペースが軍事的な色彩を強めてきたということになるだろう。無論、AIを使った経済的なインパクトや、各国の選挙への介入といった政治的なインパクトも懸念されているが、各国がサイバースペースそのものの安全保障や、サイバーシステムを使った軍事作戦を検討していることは明らかである。

従来、インターネットコミュニティは、国境を越えて接続することをモットーとし、政府による介入を忌避してきた。しかし、各国の軍事システムはインターネットと同様の技術を使ったサイバー技術に依存するようになり、政治経済システムもまたインターネットや、インターネットにつながらない部分も含むより広いサイバースペースに依存するようになっていく。そこでのセキュリティは民間だけに任せておくことはできなくなったということが、各国政府の共通理解となった。したがって、国際規範ないし条約を求める動きは今後も強まるだろう。



1996, 1997, 1998, 1999, 2000...

[インターネット白書ARCHIVES] ご利用上の注意

このファイルは、株式会社インプレスR&Dが1996年～2019年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書 ARCHIVES」として以下のウェブサイトで公開しているものです。

<https://IWParchives.jp/>

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容(技術解説、データ、URL、名称など)は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者(執筆者、写真・図の作成者、編集部など)が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元(株式会社インプレスR&D)などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&D(初期は株式会社インプレス)と著作権者は内容が正確なものであるように最大限に努めました。が、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先

株式会社インプレス R&D

✉ iwp-info@impress.co.jp

©1996-2019 Impress R&D