

国際政治とサイバー攻撃

土屋 大洋 ●慶應義塾大学大学院 政策・メディア研究科 教授

国家・個人の思惑が交錯するネット上で偽ニュースが跋扈。サイバー攻撃も実世界に混乱を来し、ネットとサイバーシステムの安全利用はますます重要な政策課題となる。

■米国トランプ政権をめぐる混乱

ドナルド・トランプ米国大統領の最側近の1人で、一時は首席戦略官兼上級顧問にもなったスティーブ・バノンがジャーナリストに暴露したところによれば、トランプ候補は2016年11月の大統領選挙に勝利するとは思っていなかったという。当選が確実になると、「放心したトランプから、起きたことが信じられないトランプ、怖気づいたトランプへと次々に変わっていった」ともいう。

当の本人さえ勝利できるとしていなかった大統領選挙の結果を左右した要因の1つがサイバー攻撃であった。

無論、国際法上のサイバー「攻撃」は、人命への危害や物理的な破壊が伴うものと定義されている。しかし、一般的には犯罪や妨害行為、スパイ活動なども含めて広い意味でサイバー攻撃という言葉が使われている。米国大統領選挙においては、トランプ候補に有利になるような情報、対立するヒラリー・クリントン候補を貶めるような情報が流され、それらの少なからぬ情報は偽ニュースといわれるものだった。

そうした偽ニュースは、アクセス広告料稼ぎの個人によるものもあれば、政府によって企図されたと疑われているものもある。その中心にいるの

がロシアである。

ロシア側の事情を探てみると、必ずしもトランプ候補を当選させようとしていたわけでもないようである。むしろ、長らくロシアの政治体制とウラジーミル・プーチン大統領を批判してきたクリントン候補を貶める、そして、クリントン候補が当選してもその選挙結果について米国民に疑念を抱かせ、米国政治そのものを揺るがすことを狙っていたと考えられる。プーチン大統領から見れば、自分に融和的な人物よりも、ロシアに対立的な人物が米国大統領になったほうが、米国と決然と対立するプーチン大統領をロシア国民向けに演出できて好都合だったはずだ。

トランプ政権が成立した後の実際の展開を見ると、米露関係そのものが疑惑の対象となり、ロシア政府と接触したトランプ政権幹部の辞任、元スタッフの逮捕へとつながり、対ロシア制裁はトランプ政権成立から1年経っても解除されていない。結局のところ、ロシア政府は米国との対決姿勢を崩していない。

■作戦領域の変化

これはサイバー戦争といえるのだろうか。従来の戦争概念では、宣戦布告がなされた後、武力が行使されることになるが、いわゆるサイバー戦争

ではそうしたことは行われていない。国家主体とも非国家主体とも簡単にはわからない誰かがサイバー攻撃を行い、その被害に何か月も気づかないことすらある。

ある行為を誰がやったのかを特定することをアトリビューションと呼ぶ。たとえば、朝鮮半島のどこかからミサイルが発射されれば、それが北朝鮮によるものだということは、ミサイルが着弾する前にアトリビュートされるだろう。しかし、サイバー攻撃の場合は、攻撃者がよほどのミスでもない限り、瞬時にはわからない。

米国のバラク・オバマ政権は従来の戦争との変化を作戦領域の変化と表現してきた。作戦領域とは戦闘空間とも言い換えられるが、作戦は戦闘よりも大きな概念で、スパイ活動のような武力攻撃以外の活動を含む。

従来の作戦領域は陸、海、空であった。それらに対応して各国で陸軍・海軍・空軍が設置されていた。しかし、4番目の作戦領域として宇宙、5番目としてサイバースペースが挙げられるようになってきた。それに呼応して各国でサイバー軍が設置されるようになってきている。陸軍、海軍、空軍と並ぶレベルでサイバー軍を設置している国はほとんどないとしても、何らかのサイバー部隊を有していると見られる国は2017年末時点で40か国程度に上る。

しかし、サイバースペースは、陸・海・空・宇宙という自然空間とは異なる人工空間である。サイバースペースの実態は、パソコンやスマホなどの各種の情報処理端末と各種の記憶装置、それらをつなぐ通信回線によって構成される機器の集成でしかない。サイバースペースを破壊するには、そうした端末や装置を不能にしたり、通信回線を妨害したりするだけでよい。陸地をミサイルで破壊したり、海洋航路を封鎖したり、制空権を奪ったりすることとは質的に異なる。

むしろ、サイバースペースは4つの作戦領域をつなぎ、覆い被さるものともいえる。軍事の世界では一時、「エア・シー・バトル」という言葉が流行した。空軍と海軍が連携しながら効果的に作戦活動を展開することを指していたが、両者の連携には通信が不可欠であり、インターネットではないにせよ、同様のデジタル機器を使った通信が不可欠である。その指揮命令システムへの攻撃もまたサイバー攻撃の一種として懸念されることになった。

そして、近年では5つの作戦領域が横断的に使われるという意味の「クロスドメイン（領域横断）攻撃」や「マルチドメイン・バトル（多領域戦闘）」といった言葉も使われるようになっていく。それが未来の戦争のあり方として各国で研究対象になっている。

さらには、ロシアが用いたような偽ニュースを流布しながら軍事的手段を行使するという「ハイブリッド戦争」も現実のものになっている。2008年のジョージア（グルジア）・ロシア間の紛争では、ロシア軍による武力行使開始とタイミングを合わせてインターネット上のサイバー攻撃も行われた。2014年のウクライナ危機においてもプロパガンダが展開された。

今後の紛争においては、たとえば、武力行使の開始と同時に、事前に調べておいた敵国の兵士たちの携帯電話に兵士の家族の緊急事態を知らせる偽のショートメッセージが送られるかもしれない。兵士たちは動揺し、作戦活動に集中できなくなるかもしれない。あるいは、インターネットを介してデマや流言が流され、国民が混乱することも想定される。

2018年1月、米国のハワイ州では、北朝鮮のミサイルがハワイに向けて発射されたとのメッセージが職員の誤操作によって住民の携帯電話に届き、一時的ながら大混乱を引き起こした。ハワイ

には、アジア太平洋の広大な地域を管轄する米国太平洋軍（PACOM）の司令部があり、兵士の家族も住んでいる。

人々の生活にインターネットが入り、主たる情報源がマスコミではなくなった結果、偽のメッセージも拡散しやすくなっている。それを敵国が活用する事態も想定しておかなければならなくなっている。

■インターネットを超えて広がるサイバースペース

インターネットに使われているサイバー技術は、インターネットを超えていろいろな場所で使われるようになった。たとえば、交通を制御するシステムや原子力発電所を制御するシステムは、インターネットに直接つながっているわけではないが、同様のコンピューターや通信システムを使う。その結果、そうしたサイバースystemが攻撃の対象にもなっている。手動ではなく、自動で安定的に重要なインフラを運用していくためには、コンピューターの利用が欠かせないからである。

そうしたシステムとインターネットとの間には「エア・ギャップ（空気の隙間）」が設定され、直接つながないことが常識とされている。しかし実際には、維持運用を目的として通信回線につながっている場合が少なくない。

かつては重要インフラを制御するシステムは「作り込み」といわれる独自のものだったが、今では汎用のオペレーティングシステム（OS）をかぶせることが多くなっている。そうしたOSの脆弱性を悪用すれば制御システムを乗っ取ることができるかもしれない。OSの脆弱性をふさぐパッチを得るために、一時的にせよ、システムがインターネットに接続される可能性もある。

あるいは、重要インフラの施設内に入り込むことができる人間がいれば、そうしたシステムに

マルウェアを侵入させることもできるだろう。重要インフラを制御するシステムを守るためにはエア・ギャップだけでは不十分で、従業員や出入り業者の人物チェックまでも行わなくてはならない。敵対する国の情報機関は、あらゆる手段を使って侵入を試みるだろう。実際、2010年に発覚したイランの核施設に対するサイバー攻撃（スタックスネット）では、非常に高度な作戦活動が展開された。

■攻撃側の視点

攻撃側に目を転じれば、その実態は多様であることがわかる。

第1に、現状に不満を持ち、社会に取り残された若者たちが、不満の捌け口としてサイバー攻撃を実行する場合がある。換金できるデータが手に入ればよいし、そうでなくても気に入らない外国の政府や企業に嫌がらせをするだけで鬱憤晴らしになるだろう。

第2に、経済的な利得を求める産業スパイがいる。国内外を問わず、知的財産を盗んだり、ライバル企業の動向を探ったりする目的で活動する人たちである。

第3に、政治的利得を求める政府機関のサイバースパイがいる。人間を使ったスパイ活動は古代からあるが、サイバーインテリジェンス（デジタルを使ったスパイ活動）は、スパイの生命を危険に曝さなくてよいという大きな利得がある。国際法上もインテリジェンス活動は必要悪としてグレーゾーンになっており、民主主義体制の国でも行われている。これがなくなることはないだろう。

第4に、各国軍による活動がある。サイバー攻撃によって直接的な死者が出る事態はまだ発生していないが、今後も行われえない保証はない。現段階では敵対する国のシステムの脆弱性を探った

1
り、実験したりするレベルで、切り札は実際の戦時まで温存されるだろう。

2
最後に、こうしたさまざまなアクターから依頼を受けてサイバー攻撃を実行する、対価をもらえれば相手を問わない、いわば「サイバー傭兵」が存在する。ダークウェブと呼ばれるサイバースペースの最深層ではそうした裏取引が仲介されている。

3
サイバー攻撃と一口にいつても、そのほとんどはサイバー犯罪であり、サイバーエスピオナージ、サイバーインテリジェンス、狭義のサイバー攻撃など多様である。それらを実行する攻撃者も多様であり、一国の政府がすべてを調整しているとは考えにくい。政府の別働隊として動いていた、純粋に民間の攻撃者もいたりする。

4 5 6 ■アトリビューションが鍵

冷戦時代の核ミサイル危機において米ソ両国の首脳が対峙し、相互に抑止を効かせることができたのは、相手が誰かはっきりしていたからである。しかし、サイバー攻撃における抑止は、相手が見えないゆえに困難である。

サイバー攻撃者をアトリビュートできれば、抑止の可能性も高まる。非国家主体も含めて効果的な懲罰・制裁が行える見込みがなければ抑止効果

は下がるが、正体を暴かれ、さらし者にされれば、サイバー攻撃を請け負うサイバー傭兵はダメージを受けるだろう。攻撃者の身元が曝されれば、現実社会での生活に困難を来したり、パスポートを持って国外に移動することができなくなったりするだろう。

■メガイベント対応

オリンピック・パラリンピック、サッカーやラグビーのワールドカップ、万国博覧会のようなメガイベントはサイバー攻撃の対象になりやすい。国家の威信や名誉を傷つけるのに格好の場になるからである。あるいは、混乱に乗じて市場取引で儲けようとする攻撃者もいるかもしれない。イベントの主催者やホスト国の政府にとっては頭痛の種である。そうしたイベントの開催費用の高騰と相まって、イベントの開催自体がリスクと考えられるようになっている。

すでに国際政治における国家主体と非国家主体は、サイバー攻撃が有用な手段であると認識している。本来、平和目的に利用されるべきインターネット、そしてその外で広がりつつあるサイバーシステムの安全な利用は、ますます重要な政策課題となっていくだろう。



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～2018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。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

©1996-2018 Impress R&D