公益財団法人日本国際問題研究所

研究レポート

「経済・安全保障リンケージ」研究会 FY2021-2 号　2021 年 8 月 3 日

ロシアのサイバー攻撃～軍事・外交における重要性

廣瀬陽子（慶応義塾大学総合政策学部教授/日本国際問題研究所客員研究員

はじめに

近年、サイバー攻撃の脅威は世界で高まっているが、特にロシアによる攻撃は、悪質で大きな被害をもたらすものとされ、またリベラル秩序を乱す脅威として認識されている。国際的には 2016 年の米国大統領選挙時のいわゆる「ロシアゲート」事件で、ロシアのサイバー攻撃や情報戦、誘導工作(インフルエンス・オペレーション)の影響力の強さが認識されるようになったと言って良いが、ロシア発のサイバー攻撃は、それ以前にも、それ以後にも行われてきた。

コロナ禍においても、ロシアはサイバー攻撃やフェイクニュースなどによる情報戦を展開し、自国にとって有利な国際的状況を生み出そうとしたことが明らかとなっている。新型コロナウイルスのワクチンを開発している研究機関や大学、製薬会社、シンクタンク、政府機関などに対するサイバー攻撃が多数確認されている他、2020 年 12 月にはロシアが同年 3 月から米ソーラーウィンズ社のソフトウェア・オリオンの脆弱性を悪用した大規模なサイバー攻撃を行なっていたことが明らかになった。その攻撃により、米国の複数の政府機関や地方政府の他、重要な民間企業等の重要情報が想像を絶する規模で盗まれたとされるが、被害は米国史上最悪レベルで、全容解明には数年を要するとも言われている。

日本にとっても対岸の火事ではなく、20 年 10 月に英外務省がロシアの軍参謀本部情報総局(GRU)が、東京五輪・パラリンピックの関係者や関係団体に対して「サイバー偵察」を実行したことを発表していたし、21 年 6 月には、日本オリンピック委員会(JOC)が 20 年 4 月にサイバー攻撃を受け、パソコンやサーバー内のデータが書き換えられて業務が停止する被害が生じ、約 60 台のパソコンやサーバーを約 3000 万円かけて交換して業務を復旧させていたことも明らかになった。

ロシアのサイバー攻撃を分析し、対応することは、喫緊の課題であることは間違いない。本稿では、ロシアにおけるサイバー攻撃の位置付け、その特徴などを明らかにし、今後の課題について検討する。

ロシアにおける「サイバー」の位置づけ

ロシアにおける情報戦やそのサイバー領域における役割などは、国家安全保障戦略(2015 年版及び 2021 年版)、対外政策概念(2016 年発出)、情報セキュリティドクトリン(16 年)、軍事ドクトリン(14 年)、情報空間におけるロシア連邦軍隊の活動に関する概念的見解(16 年)などの戦略的政策文書で論じられているが、ロシアにおいては、サイバー戦や情報技術戦は、「情報対立」の包括的概念の一部に過ぎず、情報の対立において優位性を獲得するために使用される方法の一つだと位置付けられている[i]。なお、ロシアの戦略文書においては、「サイバーセキュリティ」という用語は用いられておらず、代わりに「情報セキュリティ」という言葉が使用され、デジタルネットワークの保護のみならず、認知の保全もその対象とされる[ii]。

そして、サイバー攻撃はロシアのいわゆる「ハイブリッド戦争」[iii]において、極めて重要な位置を占めている。ハイブリッド戦争とは、政治的目的を達成するために、軍事的脅迫とそれ以外の様々な手段(政治、経済、外交、サイバー攻撃、プロパガンダを含む情報・心理戦などのツールのほか、テロや犯罪行為も)が組み合わされた、非正規戦と正規戦を組み合わせた戦争の手法で、決して新しいものではないが、2014 年のロシアのクリミア併合や東部ウクライナの危機において世界の脅威として強く認識されたという事情がある。サイバー攻撃は、ロシアのマルチドメイン作戦の一部として重要な意義を持っている。

なお、ロシアにおける「ハイブリッド戦争」はそれ自体が戦略というわけではなく、作戦であり、クリミア併合を経て、軍事コンセプトからロシアの外交政策の理論に準じるものに変わった[iv]。そして、それは同様にサイバー攻撃、そしてサイバー攻撃と組み合わせることによって大きな効果を生み出す情報戦についても言えることであろう。

ロシアのサイバー攻撃の実行者

ロシアのサイバー攻撃や情報戦は、国家などが意図を持って行うもの、犯罪集団によるもの、愛国者によるもの、民間企業などによるものと、さまざまな主体に担われているが、近年の趨勢から見るに特に厄介なのは、国家が関与するものと犯罪集団によるものだと言える。

国家が関与するものとしては、まずロシア連邦軍に 1000 人規模の 15 のサイバー部隊が設置されているが、世界から危惧されているのはインテリジェンス系組織による攻撃、すなわち GRU(ロシア連邦軍参謀本部情報総局)、 FSB(連邦保安局)、SVR(連邦対外情報局)が関わるサイバー攻撃である。それらの規模と被害は甚大であり、事例は枚挙にいとまがない。

GRU の指揮下にあるサイバー集団は APT 28 などと呼ばれ、2008 年から活動している。敵対する国・旧ソ連諸国の航空宇宙、防衛、エネルギー、政府、メディア、国内の反体制派などをターゲットとし、2020 年に JOC を狙ったのも GRU だとされる。フィッシングメッセージとなりすましウェブサイトなどの手段を多用するが、情報を盗み、それを広く暴露して相手にダメージを与える手法から、攻撃の事実が明らかになりやすく、それ故に多くの刑事告発を受けてきた。

FSB の指揮下にあるとされる Turla APT などと呼ばれるサイバー集団、SVR の指揮下にあるとされる APT29 などと呼ばれるサイバー集団は、2014 年頃から国際的に認知され、2016 年米国大統領選挙、2020 年の米国などに対する大規模サイバー攻撃など大規模な攻撃を行うのが特徴である。セキュリティを巧妙にすり抜け、クレムリンに役立つ情報収集を行うが、それを暴露することはしないため、表面化しづらいとされている。

その他、多くの政府系ハッカー集団の活動が確認されている[v]。

そして、近年、深刻な問題となっているのが、ロシアを拠点にするサイバー犯罪集団による攻撃である。特に、2020 年から 21 年にかけてはロシアを拠点にする犯罪集団「REvil」や「ダークサイド」による大規模なランサムウエア(身代金ウイルス)攻撃が目立つようになった。特に、21 年 5 月初旬の「ダークサイド」による米・パイプライン大手のコロニアルパイプラインに対するランサムウエア攻撃、5 月末の「REvil」による世界最大の食肉業者 JBS(本社・ブラジル。米国に大規模工場多数)に対するランサムウエア攻撃、7 月初旬の「REvil」による IT システム管理サービス提供会社 Kaseya の VSA ソフトウエアの脆弱性を悪用したサプライチェーンランサムウエア攻撃などは、極めて深刻な被害をもたらした。

このようなロシアを拠点にする犯罪集団によるサイバー攻撃について、米国はロシア政府に責任を問うが、ロシアサイドは犯罪集団とは無関係であり、関係を示す証拠もないという立場を取る。だが、GRU などが犯罪集団と繋がっているという専門家の意見は少なくなく、報酬が支払われている、仮に有罪になった場合の刑罰が大幅に減刑されているなどの指摘もなされている[vi]。また、英国の国際戦略研究所(IISS: The International Institute for Strategic Studies)もサイバー攻撃の資金不足の故に、国家がサイバー犯罪専門家や愛国的ハッカーも利用していると指摘している[vii]。

ロシアのサイバー攻撃の特徴

ロシアのサイバー攻撃は以下のような特徴を持つ。

まず、国家支援型のサイバー攻撃が特に強い深刻な影響を及ぼしているということである。なお、攻撃を行うロシアの最初の国家支援型のサイバー攻撃は、米国の兵器に関する情報を狙った 1996 年の「Moonlight Maze」だと見られているが、2007 年にエストニアに行った大規模なサイバー攻撃(タリン事件)や 2016 年の米国大統領選挙におけるサイバー攻撃が特に甚大な被害をもたらしたといえる。なお、それらハッカー集団間の横の連携や協力関係がないことも特徴である。

また、高いスキルがあり、ネットワークへの侵入から PC やデバイスの乗っ取り、システムをダウンに至るまでの作業をわずか 18 分で完了できるとされ、これは世界最速である。

だが、防衛力が弱く、米国の防衛手法を模倣する形での対応しかできていないとされる。そのため、ロシアのサイバー攻撃を何度も受けているジョージアのコンピューター緊急対応チーム(CERT: Computer Emergency Response Team)がサイバートラップで反撃し、ロシアの攻撃者を丸裸にしたということもあった[viii]。なお、ジョージアの事例は、攻撃による防衛の重要事例だと言える。

攻撃の内容が目的や相手によって変わることも特徴である。その特徴は、特にハイブリッド戦争との絡みでより顕在化する。まず、欧米諸国の政治を混乱させることが目的の場合は、情報の入手・拡散という手段が目立つ。だが、ロシアが影響圏と考える旧ソ連諸国に対する攻撃が中心となるが、軍事的な戦闘を展開しながら同時にサイバー攻撃を行う場合や相手国への懲罰的な意味合いが大きい場合には、政府関連、インターネット網や電力システム、銀行システムなど、重要インフラを狙うことが多い。

結びにかえて

このように、ロシア発のサイバー攻撃は、情報戦などのインフルエンス・オペレーションとの相乗効果も得ながら、相手国の政治に影響を与えたり、はたまたランサム攻撃を行ったりして世界の社会・経済に大きな影響を与えてきた。

米国のバイデン政権は、サイバー領域でもロシアに対して厳しい姿勢をとっており、21 年 6 月 16 日に行われたバイデン・プーチン両大統領による初の米露首脳会談でもサイバー問題は重要な論点になった。同会談で、バイデン氏はロシアが責任を取るべきだという主張を展開した上で、重要インフラを攻撃の対象から外すべきだとして、16 分野(化学、商業施設、通信、重要な製造分野、ダム、防衛産業基盤、緊急サービス、エネルギー、金融サービス、食品・農業、政府施設、医療・公衆衛生、情報技術、原子炉・核物質・核廃棄物、輸送システム、水・廃水システム[ix])の重要インフラを記したリストをプーチン氏に手渡した[x]。だが、プーチン氏はロシア政府のサイバー攻撃への関与を改めて否定し、記者会見でもロシアへのサイバー攻撃のほとんどは米国・カナダ発だなどと発言し、両国の隔たりの大きさが明らかになった一方、両国間の専門家協議を行っていく事では合意ができ、それがすぐに実行にうつされたことは、サイバー問題での国際協調に向けての明るい一歩と言えるだろう。

また、日本もサイバー領域における国際協力[xi]を進める一方、リテラシー能力やサイバー教育の拡充を行って国民の意識を強化しながら、サイバー領域での優秀な人材の確保、ホワイトハッカー養成など専守防衛にとどまらずに攻撃しながら防衛する姿勢の強化を図るなど、多面的なサイバー対策を構築してゆくことが喫緊の課題であろう。

---

[i] Janne Hakala, Jazlyn Melnychuk (2021), *Russia's Strategy in Cyberspace,* NATO StratComCOE, pp.5-6.

[ii] Nicu Popescu, Stanislav Secrieru eds. (2018), *Hacks, leaks and disruptions - Russian cyber strategies*, EUISS, p. 17.

[iii] ロシアのハイブリッド戦争については、拙著『ハイブリッド戦争　ロシアの新しい国家戦略』(講談社新書、2021 年)を参照されたい。

[iv] Renz, Bettina and Hanna Smith (2016), *Russia and Hybrid Warfare - Going Beyond the Label,* Aleksanteri Papers, 1/2016.

[v] 以上、廣瀬(2021)および Hakala, Melnychuk (2021)。

[vi] Hakala, Melnychuk (2021)。

[vii] IISS (2021), *Cyber Capabilities and National Power: A Net Assessment*, Research Papers.

[viii] 佐藤仁「ロシア・グルジアのサイバー戦争：サイバー反撃による秘匿性の崩壊」『情報通信総合研究所 InfoCom ニューズレター」(2012 年 12 月 14 日)(https://www.icr.co.jp/newsletter/global_perspective/2012/Gpre2012103.html)。

[ix] 本 16 セクターは、米国サイバーセキュリティ・インフラストラクチャ・セキュリティ庁(CISA)が示す「重要インフラセクター(https://www.cisa.gov/critical-infrastructure-sectors)」[2020 年 10 月 21 日に更新]に合致するため、本会談のために用意された項目ではなく、従来の米国の「レッドライン」であると言える。

[x] ただし、サイバー問題で、このような「レッドライン」を提示することの意義については国際的にも賛否がある。

[xi] ロシア周辺国では、NATO や EU 等の国際協力によってハイブリッド戦争やサイバー攻撃に対抗するシステム作りが進んでおり、フィンランドに「ハイブリッド脅威対策センター」(The European Centre of Excellence for Countering Hybrid Threats[Hybrid CoE])、エストニア「サイバー防衛センター」(NATO Cooperative Cyber Defence Centre of Excellence)、リトアニアに「エネルギー安全保障センター」(NATO Energy Security Centre of Excellence)、ラトビアに「戦略的コミュニケーションセンター」(StratCom：Strategic Communications Centre of Excellence)が設置され、重層的な危機管理体制がとられている。エ

ストニアは 2007 年のロシアから大規模なサイバー攻撃によって大打撃を受けたことを教訓に、国民にサイバー教育を徹底し、「サイバー衛生」(サイバー攻撃者に利するような習慣を変えて、個人が自分の身を守る)が国民に浸透するようにして、サイバー防衛を強化している。