ウクライナIT軍「サイバーハッキング」の衝撃

～攻撃対象となるロシア国産 SNS や動画共有サービス～

ライフデザイン研究部 主席研究員 柏村 祐

1.ウクライナIT軍が行うサイバー攻撃の多様化

ロシアによるウクライナ侵攻が始まり 3 か月が経過した。筆者は以前、ウクライナ政府がウクライナ IT 軍を立ち上げ、ロシアに対し DDoS 攻撃と呼ばれるサイバー攻撃を行っていることに触れ、その手法の拡大により誰もが簡単に参加できる戦場がサイバー空間に広がっていると述べた。また、「ロシア人への声明」という情報伝達活動を通じて、ウクライナ IT 軍がロシア国内の反戦機運を高める情報戦を展開していることも紹介している（注 1、注 2）。

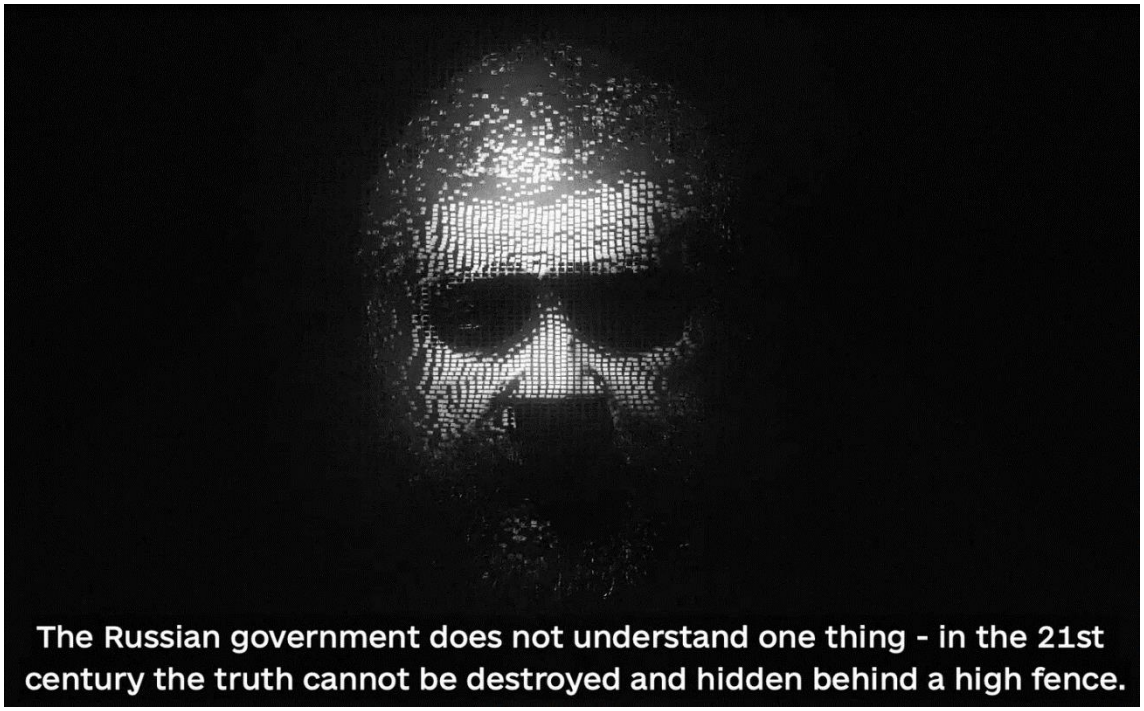
そのウクライナ IT 軍は、これらとは別のサイバー攻撃として、ロシア国民が利用するロシア国産 SNS や動画配信サービスへの「サイバーハッキング」を行っている。

2.ウクライナIT軍が行うサイバーハッキング

ウクライナ IT 軍が実践するサイバーハッキングの状況は、公式 SNS で確認することができる。具体例の 1 つとして、ロシアを代表する動画共有サービス Rutube への攻撃が挙げられる。2022 年 5 月 15 日に公開された、このサイバーハッキングの詳細を説明した動画は、ウクライナ IT 軍の公式 SNS に加入した人が閲覧できる。

この動画の中で、人間の顔を模倣したウクライナ IT 軍の司会者は、くぐもった声で話かけてくる。「Rutube の管理者は、5 月 8 日から 9 日までの夜の勤務シフトを一生忘れられないだろう。管理者は、午前 4 時ごろ、システムの異常動作に気づき、チェックし始めた。しかし、管理者が次に驚いたのは、システムの制御ができないことだった。パスワードが使えなくなっていたのだ」と述べている。この成果報告は、ウクライナ IT 軍が Rutube に対するサイバーハッキングに成功し、その操作権限がウクライナ IT 軍に奪われてしまったことを意味する。これに対して、Rutube 側は、サーバールームへ赴き直接データ管理権限を取り戻そうとするが、既にウクライナ IT 軍はデータを盗み出すことに成功したとし、「Rutube の管理者が必死になっているにもかかわらず、私たちが管理者権限を取得し、プラットフォームを完全に制御できたという証拠がすべて揃っている」という発言とともに、サイバーハッキングに成功した状況を示すデータが動画上で映し出される。この動画の最後で、人間の顔を模倣した司会者は「ロシア政府は、21 世紀において真実を無かったものとし、隠すことはありえないということを、ひとつも理解していない」と締めくくる（図表 1）。

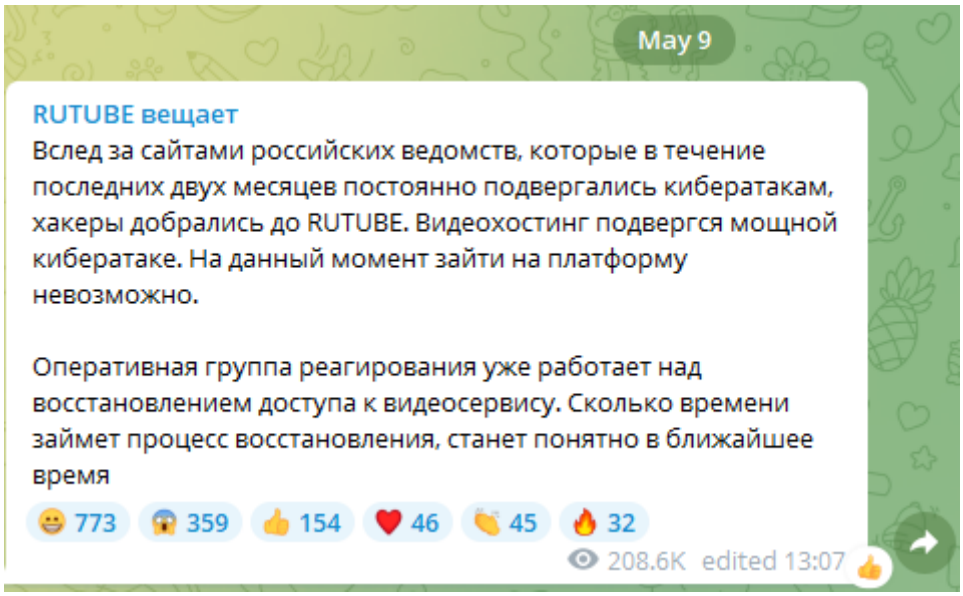
図表１　メッセージを伝える動画の司会者



資料：TelegramSNS「IT army is on air」より

この動画はウクライナ IT 軍が一方的に配信したものだが、この動画で示されたサイバーハッキングの信憑性を高める声明が、2022 年 5 月 9 日に Rutube 側から発表されている。その内容は「この 2 ヶ月間、絶えずサイバー攻撃を受けているロシア政府機関のウェブサイトに続き、ハッカーは Rutube にたどり着いたのです。動画中継サイトが激しいサイバー攻撃を受けています。現在、プラットフォームへのアクセスは不可能です」となっており、動画共有サービスが停止している原因がサイバー攻撃であると認めている。（図表 2）。

図表 2　Rutube 公式 SNS による発表



資料：TelegramSNS「https://t.me/rutube/4173」

ロシアによるウクライナ侵攻を契機に始まったサイバー空間における情報戦は、それが実際に行われたのか、それともフェイクニュースなのかを検証することは難しい。Rutube へのサイバーハッキングの事例は、ウクライナ IT 軍がサイバー攻撃を行ったことを発表する一方で、ロシア側が攻撃を受けたことを認めたことにより、その信憑性は高いと考えられる。5 月 9 日はロシアの対ドイツ戦勝記念日であり、そのパレード映像がハッキングによって Rutube で公開できなかったことは、ロシア国内への情報発信を妨害することにつながっている。

また、ウクライナ IT 軍は、ロシアに対するサイバーハッキングの別の事例として、2022 年 4 月 7 日に行ったハッキングの状況を公開している。その内容は、ロシア国産の SNS であるロスグラムにサイバーハッキングを行い、利用者の個人情報を抜き取ったというものだ。ウクライナ侵攻が開始されて以降、ロシアでは国内の情報統制を強化すべく海外 SNS を閲覧できない状況が続いている。その代替策としてロスグラムが開発され、3 月 28 日から利用が開始される予定となっていた。ウクライナ IT 軍は、3 月中旬にロスグラムのネットワークに侵入してそのコピーサイトを作り、ロスグラムの管理者のふりをして、本物のロスグラム登録者に対し手続きを装ったメッセージを送信し、登録者から個人情報を抜き取っている。その証拠として、ウクライナ IT 軍は、ハッキングしたロシア人の個人情報を 2022 年 3 月 29 日にツイッター上で全世界に公開している（図表 3）。公開後に筆者がその情報を確認したところ、名前、電話番号、メールアドレスが掲載されていた。ただし、2022 年 5 月 20 日現在、ツイッター上からその情報は削除されている。

図表 3　ウクライナIT軍がハッキングした Rosgram の加入者情報

資料：TwitterSNS「https://twitter.com/sudormRF6/status/1508783518645735429」より筆者ぼかし加工

3.戦時のサイバー攻撃をどう捉えるべきか

今回のウクライナ侵攻では、兵士や兵器による物理的な戦いだけではなく、サイバー空間における戦争が拡大していることがうかがえる。未だ先行き不透明な状況が続いており、このまま戦闘が長期化すれば、ウクライナIT軍は、本稿で見たようなサイバーハッキングを巧みに利用したサイバー攻撃を拡大させる可能性もある。そしてそれは、今回見たように、その場がサイバー空間であるがゆえに、関与者が軍なのか、民間なのか境界線があいまいになっている現実をさらに浮き彫りにするだろう。

政府による情報統制が進むロシア国内では、ロシア国産のSNSや動画共有プラットフォームがロシア国民の情報源の１つとなっている。今回のウクライナIT軍によるサイバーハッキングは、その動画共有サービスの操作権限をはく奪したり、SNSを利用するロシア人の個人情報を取得したものだ。

そもそも平時においてハッキングは犯罪行為にあたる。ウクライナIT軍によるサイバーハッキングは、侵攻に対するロシアへの報復として行われているものかもしれないが、戦時のサイバー攻撃、そして民間人が参加している可能性もある行為をどう捉えるべきなのか、今後様々な分野で国際的な議論が求められる重要な課題といえるであろう。

【注釈】

1) ウクライナ IT 軍「サイバー攻撃」の衝撃～誰もが簡単に参加できる DDoS 攻撃が拡大する世界～
https://www.dlri.co.jp/report/ld/186918.html

2) ウクライナ IT 軍「ロシア人への声明」の衝撃～あなたが知らないウクライナ IT 軍による情報伝達活動～

https://www.dlri.co.jp/report/ld/187785.html