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～

ライフデザイン研究部 主席研究員 柏村 祐

1. 情報発信に積極的なウクライナ政府

ロシアのウクライナ侵攻が始まり 2 か月以上が経過した。当初は早期に決着すると想定されていたが、未だその行く末は不透明な状況となっている。侵攻当初から、ウクライナ政府は公式ホームページや SNS を通じ情報発信に力を入れてきた。その中でも特に SNS を通じた発信を行っている人物として、ゼレンスキー大統領やデジタル省のフェドロフ大臣が挙げられる。発信される情報は、ウクライナ国内のみならず世界にも向けられており、ロシアによる侵攻の状況、それに対するウクライナの対応、世界に向けた軍事・人道支援の呼びかけ、国民に対する情報提供などである。

今回の侵攻では、現実空間の陸・海・空で繰り広げられる戦車やミサイルによる戦闘に加え、仮想空間におけるサイバー攻撃も活用されている。ロシアのサイバー攻撃に関しては公式な発信がないため、その実態を確認することは難しい。一方のウクライナによるサイバー攻撃についても全貌は明らかではないが、ウクライナ政府が唯一公式に発信しているサイバー攻撃部隊として、IT ARMY of Ukraine（以下ウクライナ IT 軍）が挙げられる。その存在が広く知られることになったきっかけは、ウクライナ政府デジタル省のフェドロフ大臣が、ツイッターを通じて、ロシアに対するサイバー攻撃を行うよう国内外へ呼び掛けたことにある。フェドロフ大臣は、「我々は IT 軍を編成しています。デジタルの才能を持つ人たちを求めています。すべてのタスクはここ（https://t.me/itarmyofurraine）にあります。すべての人のためのタスクがあります。私たちはサイバーの最前線で戦い続けます。最初のタスクは、サイバースペシャリスト向けのチャネルです」（注 1）と発言し、SNS 上にウクライナ IT 軍を立ち上げている。

そこで本稿では、ウクライナ政府が主導するウクライナ IT 軍によるサイバー攻撃の状況を確認したうえで、それをどう捉えるべきかについて考察する。

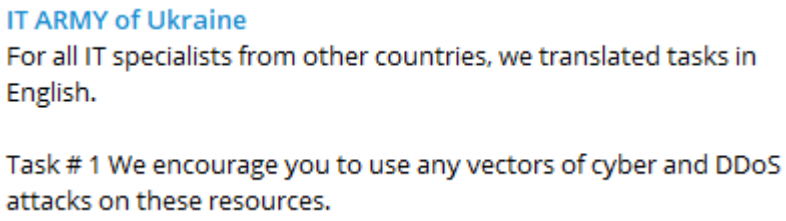
2. ウクライナIT軍のサイバー攻撃の概要

ウクライナ IT 軍のサイバー攻撃は、ロシアによるウクライナ侵攻に対抗するために始められた。ロシアの政府や行政サービス、金融、情報通信、医療、電力などの重要インフラを遠隔地からサイバー攻撃し、ロシアの国民生活、社会・経済活動を混乱させることを目的としている。

実際筆者は、ウクライナ IT 軍の SNS に登録し、ウクライナによるサイバー攻撃の

実態を探ってみた。ウクライナ IT 軍が 2022 年 2 月 27 日に SNS 上で投稿した内容は、「仕事その 1、これらの攻撃対象に対するサイバー攻撃として DDoS 攻撃を使用することをお勧めします」と記載され（図表 1）、その下には、攻撃対象としてロシアの事業会社、銀行、政府・行政機関のウェブサイトのアドレスが掲示されている。

図表 1　ウクライナ IT 軍がサイバー攻撃を勧める投稿画面



資料：Telegram HP「https://t.me/itarmyofukraine2022/5」

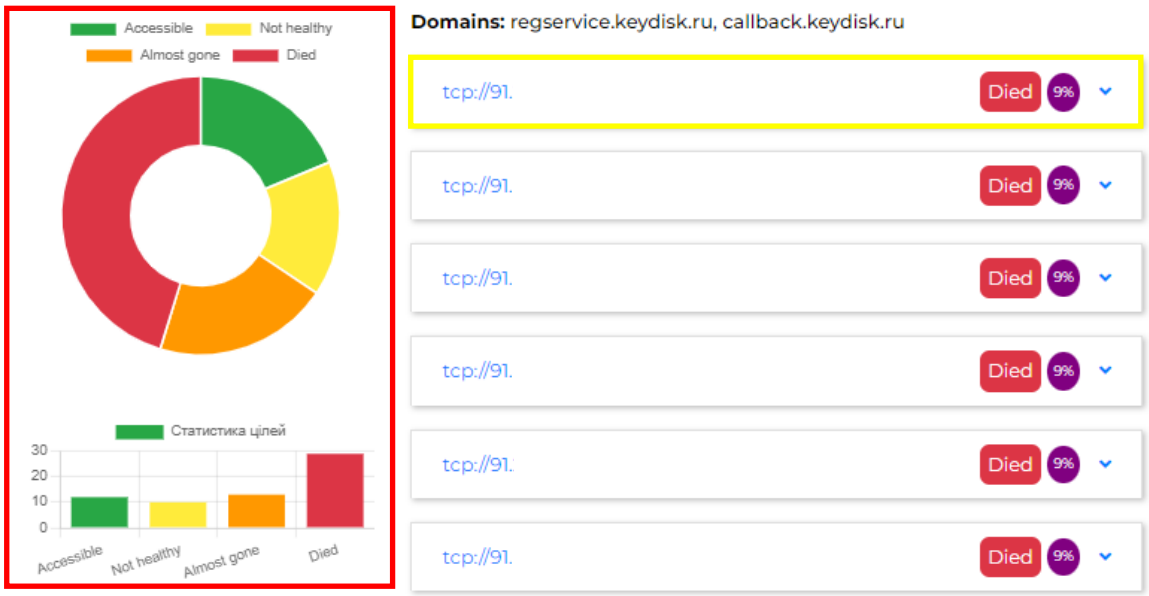
さらにウクライナ IT 軍は、攻撃対象であるロシア関連の事業体のホームページアドレスに対する「サイバー攻撃方法」、「サイバー攻撃結果」についての情報を開示している。

最初に「サイバー攻撃方法」について確認してみよう。サイバー攻撃には様々な手法が存在するが、ウクライナIT軍は、DDoS攻撃（ディードス攻撃と読む）と呼ばれる攻撃方法を紹介している。DDoS攻撃とは、Distributed Denial of Service attackの略称であり、対象となるウェブサイトに対して、複数のコンピューターから過剰なアクセスやデータを送付するサイバー攻撃の1つである。ウクライナIT軍が紹介するDDoS攻撃の方法は、仕事でコンピューターを利用している人であれば、容易に実行できるものである。ウクライナIT軍は、具体的なDDoS攻撃として、2022年3月24日にテレグラム上で「1,000本の針による死」という攻撃方法（注2）を、また2022年3月29日には「リベレーター」という攻撃方法を紹介している（注3）。

さらにウクライナ IT 軍は、これらのサイバー攻撃を通じて得られた「サイバー攻撃結果」を開示している。ウクライナ IT 軍が定めた DDoS 攻撃の目標は、2022 年 4 月 23 日時点で 64 機関に上っている。結果を確認するために、世界中の 21 台のサーバーから同時に、対象である 64 機関のウェブサイトの動作確認が 10 分ごとに行われている。対象のウェブサイトの状況は「利用可能」、「まだ動いている」、「ほとんど動いていない」、「動いていない」、「判定不能」に判別されるが、ウクライナの DDoS 攻撃が成功すれば、「ほとんど動いていない」「動いていない」と判定される機関が増加する。一方、DDoS 攻撃がうまくいっていない場合は、「利用可能」、「まだ動いている」と判定される機関が増えることになる。ウクライナ IT 軍の目標は、攻撃対象を「動いていない」にすることである。2022 年 4 月 23 日時点の「サイバー攻撃結果」の状況を確認したところ、64 機関の内訳は、「利用可能」12 機関、「まだ動いてい

る」10機関、「ほとんど動いていない」13機関、「動いていない」29機関となっている（図表2赤枠）。また、個別のウェブサイトの稼働状況も確認できる。例えば「tcp://91.」で始まるウェブサイトは「動いていない」ことがわかる（図表2黄枠）。

図表2　可視化されるサイバー攻撃の判定結果



資料：ItArmyofUkraine HP「https://itarmy.com.ua/check/?lang=en」

3. ウクライナによるサイバー攻撃の意味

以上みてきたように、ウクライナIT軍によるサイバー攻撃は、現実空間における攻撃と同様に攻撃目標が明確化され、また、攻撃した結果についてもその可視化が進んでいる。

今回実践されているサイバー攻撃は、ロシアによる侵攻からウクライナ政府が国を守るために始めたものだが、これについて筆者は、「サイバー攻撃手法の拡大により、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事実」を認識することが重要であると考える。

従来、サイバー攻撃と言えば、国家が主体であるものや一部のハッカーによるものと考えられてきた。しかし、今回ウクライナIT軍が実践しているDDoS攻撃は、ウクライナの民間人や国外の外国人が、自分のパソコンでサイバー攻撃を実践できる「場」を提供しているものといえる。このようなサイバー攻撃は、物理的に離れていても狙いを定めて攻撃することが可能であり、加えて誰もが簡単に参加できる。民間人やウクライナ国外の外国人がロシアの政府機関、民間事業会社、銀行などへのサイバー攻撃に加わるのは、犯罪に結びつくだけでなく、まさに戦争に参加する行為であり許されるものではないが、世界の民間人を巻き込んだサイバー空間における新たな戦場が

生じているという事実は認識すべきであろう。

サイバー攻撃は国家や一部のハッカーが行うことという従来の通念に囚われないウクライナIT軍によるDDoS攻撃は、混沌とする世界において「サイバー攻撃手法の拡大により、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事実」を示している。世界の安全が急速に脅かされる今、我が国においても、サイバー空間における攻撃や防御について、早急に調査研究していくことが求められるだろう。

【注釈】

1) twitterHP より筆者和訳
https://twitter.com/fedorovmykhailo/status/1497642156076511233
2) TelegramHP より
https://telegra.ph/Death-by-1000-needles-03-17
3) TelegramHP より
https://t.me/itarmyofukraine2022/245