「第五の主戦場」サイバー攻撃応酬の脅威

なぜ、ロシアはウクライナのシステムが全面ダウンするような攻撃を避けているのか。「サイバー義勇兵」や複数の国際ハッカー集団の「参戦」がもたらす未曾有の事態とは。陸、海、空、宇宙に続く「第五の戦闘領域」で戦われるハイブリッド戦、その実態に迫る。

NTTチーフ・サイバーセキュリティ・ストラテジスト
松原実穂子
まつばら　みほこ　ジョンズ・ホプキンズ大学大学院卒。防衛省などを経て、二〇一八年NTTに入社。サイバーセキュリティに関する情報発信と提言に努める。著書に『サイバーセキュリティ　組織を脅威から守る戦略・人材・インテリジェンス』。

昨年末以来、ウクライナ情勢が緊迫化する中、ウクライナ政府だけでなく世界が警戒を強めてきたのが、ロシアからのサイバー攻撃である。二〇一四年のクリミア併合時に見られるように、ロシアは軍事攻撃に情報操作やサイバー攻撃などを組み合わせ、戦略目標を達成する「ハイブリッド戦」を今までも実行してきたからだ。

軍事侵攻前から始まったサイバー攻撃

軍事侵攻の始まる四〇日ほど前の一月一三日、ウクライナの外務省、国防省など約七〇のウェブサイトがサイバー攻撃を受けて改ざんされてしまった。ロシア語、ウクライナ語、ポーランド語で「恐れよ、そして最悪の事態に備えよ」とのメッセージが書き込まれており、ウクライナに脅しをかけて、混乱をもたらそうとした攻撃だったと考えられる。ウクライナ政府は、ロシアによるサイバー攻撃だったとして非難している。

さらに軍事侵攻の約一〇日前の二月一五日、ウクライナ国防省や軍参謀本部などの政府のウェブサイトが「DDoS（ディードス）攻撃」を受け、一時ダウンした。ウクライナの国立貯蓄銀行や最大の商業銀行であるプリヴァト銀

行もＤＤｏＳ攻撃のため、アプリやオンライン決済が二時間使えなくなっている。

「ＤＤｏＳ攻撃」とは、対象のサーバーやウェブサイトに大量のデータを送りつけることで過剰な負荷をかけ、ダウンさせてしまうものだ。前回のウェブサイトの改ざんに比べ、二月一五日のサイバー攻撃の方が、行政サービスや市民生活に与える影響が大きい。

ウクライナのミハイロ・フョードロフ副首相兼デジタル変革相は、この攻撃が「時間をかけてじっくり準備された」「未曾有の」規模のものであったと指摘し、サイバー攻撃はウクライナの不安定化とパニックを狙ったものだろうと見ている。

ＤＤｏＳ攻撃からわずか三日後の二月一八日、米英両政府は、ウクライナへの攻撃元を公表した。ロシア連邦軍参謀本部情報総局（ＧＲＵ）がウクライナの銀行へのＤＤｏＳ攻撃を行ったと述べた上で、ウクライナの主権を無視した行為は受け入れ難いと非難している。また、オーストラリア政府も、英米政府に呼応する形で二月二〇日に同様の非難声明を出した。

従来の米国政府であれば、サイバー攻撃が行われてから攻撃者の身元の発表まで数ヵ月から一年以上もの時間を要していたのに対し、今回は、わずか三日間と史上最速である。しかも単独での発表ではなく、同盟国と協調し、攻撃国に早急に責任を負わせ、世界に向けて断固とした姿勢を取ることで抑止力を高めたいとの強い意志が示された。

軍事侵攻とともに行われたサイバー攻撃

二月二四日、ロシアがウクライナへの軍事侵攻を始めたのとタイミングを合わせ、少なくとも二種類のサイバー攻撃がウクライナに行われた。

まず、軍事侵攻の前日の二月二三日、「ワイパー」と呼ばれるコンピュータウイルスがウクライナの金融機関、ウクライナ政府との契約業務のあるラトビアとリトアニアの企業で見つかった。このコンピュータウイルスは業務妨害を目的としたもので、感染したシステムからデータを削除し、そのシステムを使えなくしてしまう。

スロバキアのサイバーセキュリティ企業「ＥＳＥＴ」の調査によると、この新規のコンピュータウイルス「HermeticWiper」が作られたのは、昨年一二月二八日だった。軍事侵攻の少なくとも二ヵ月前から、ハイブリッド戦が準備されていたものと考えられる。

軍事侵攻当日、サイバー攻撃の第二波が押し寄せた。ウ

クライナ議会が緊急事態宣言の発出について話し合い始めたのとほぼ同時に、大規模なＤＤｏＳ攻撃が、ウクライナ内閣、外務省、インフラ省、教育科学省、国立貯蓄銀行とプリヴァト銀行などのウェブサイトに仕掛けられ、それらのウェブサイトが一時ダウンしてしまった。軍事侵攻時のウクライナ側の混乱増幅が目的と考えられる。

ロシアはあえてサイバー攻撃を抑えた？

二月二四日以前は、ロシアがもしウクライナに軍事侵攻することがあれば、まずウクライナの通信ネットワークにサイバー攻撃を仕掛け、通信サービスなどの重要インフラをかなりダウンさせるのではないかと見られていた。だが、重要インフラへのサイバー攻撃は発生しているものの、その規模は今のところ抑制されたものとなっている。

イスラエルのサイバーセキュリティ企業「チェックポイント」によると、二月二四日にロシアがウクライナに軍事侵攻を開始して以降の三日間で、ウクライナの政府機関と軍へのサイバー攻撃件数は一九六％増加した。しかし、これは事前に予想されていたよりもかなり少ない。三月二日付の『ＭＩＴテクノロジー・レビュー』誌が指摘しているように、以前のロシアであれば、ウクライナに破壊的なサイバー攻撃を仕掛けていたのに対し、今回の軍事侵攻では今のところ、サイバー攻撃よりも伝統的な地上戦に注力しているように見える。

実際、三月八日、米国家安全保障局（ＮＳＡ）長官兼サイバー軍司令官であるポール・ナカソネ陸軍大将は、「ロシアは、ここ数週間の間にウクライナに対して数回のサイバー攻撃を行ったが、戦争が始まる前に米国が予想していたほどのハッキングはまだ起きていない」と米下院情報委員会公聴会での証言で認めている。ナカソネ司令官は、ロシアのサイバー攻撃被害が抑えられている理由として、ウクライナ側の防御、ロシア側が直面したいくつかの課題、そして「他の人々」の活躍による被害の阻止があったと説明した。

実は二〇一五年一二月、ウクライナへのロシアによるサイバー攻撃で停電が発生して以来、米国政府はウクライナに対し、多額のサイバーセキュリティ強化支援を行ってきた。二一年一〇～一一月には、米陸軍サイバー部隊、米国政府の委託業者と米国の民間企業社員がウクライナを訪れ、ロシアが地上戦と同時並行して仕掛けてきそうなサイバー攻撃に備えるための支援を行ったという。英「フィナンシャル・タイムズ」紙によると、コンピュータウイルスが既にウクライナのシステム内に潜り込んでいないか調

べ、ウクライナの重要インフラをサイバー攻撃から守るための協力が行われた。

ウクライナや米国を含む他国の防御努力に加えて、もう一つ考えられるのが、ロシアがあえて、通信ネットワークへの大規模損害を避けたという説である。二月二八日付の米「ワシントン・ポスト」紙（電子版）は、ロシアからのサイバー攻撃でウクライナの通信ネットワークの大部分がダウンさせられていない理由として、いくつかの仮説を紹介した。

第一に、軍事侵攻すればウクライナがすぐに屈服するものと、ロシアは当初思い込んでおり、占領後に自分たちが使う通信ネットワークを維持しておきたかったからだというものだ。第二に、通信がダウンすると、かえって重要な戦時情報収集をロシアができなくなってしまうので、それは避けたのではないかとの指摘もある。

今後懸念されるシナリオ

①業務妨害型攻撃被害の世界拡大

今後、日本を含む各国が警戒しなければならないサイバー攻撃の種類は、主に三つある。

第一に、ウクライナ軍や政府がロシアの軍事侵攻に対応するのを妨害し、国内でパニックを引き起こすため、ウクライナ国内の電力、交通、金融、通信などの重要インフラ企業に対し、ワイパーを使って業務妨害型のサイバー攻撃を仕掛けることだ。その際、ウクライナを狙って仕掛けられたサイバー攻撃だったとしても、コンピュータウイルス感染被害がドミノ式に世界へ広がってしまうシナリオも考えられる。

その証左が、二〇一七年六月に起きた「ノットペトヤ」と呼ばれるワイパー型コンピュータウイルスによるサイバー攻撃である。ウクライナの政府機関や電力・通信などの重要インフラ企業が被害を受けたほか、最終的には世界六五ヵ国に感染が拡散、総被害額は一〇〇億ドル（約一兆一五五〇億円）にも及んだ。

米英政府は一八年二月、ロシアによる犯行だったとして非難したが、ロシア政府は関与を否定している。

しかもロシアはその後、サプライチェーンを悪用して、被害を広げる攻撃手法を編み出した。世界的に広く使われているサービスや製品にサイバー攻撃を仕掛ければ、サプライチェーンを伝わって、感染被害をドミノ式にさまざまな国の顧客企業や政府機関へと拡大できる。

この種のサイバー攻撃を警戒する欧州連合（EU）加盟

国は、大規模なサイバー攻撃へのEUの対応能力を確かめるため、一月中旬から六週間にわたってサイバー演習を行っていた。

②制裁への報復攻撃

第二のシナリオは、ロシアの軍事侵攻に対する制裁措置を取った国々に対し、金融機関などの重要インフラへ報復としてサイバー攻撃を仕掛けるものだ。プーチン大統領は、三月五日、欧米諸国の制裁措置は宣戦布告に等しいと述べているため、懸念が広がっている。

報復で使われるかもしれないサイバー攻撃の手法として警戒されているのが、ランサムウェア攻撃のほか、ワイパー攻撃、ウェブサイトをダウンさせるDDoS攻撃である。サイバー攻撃を受けた国の社会経済活動が中断し、安全保障上のリスクとなり得、ウクライナ危機への対応・支援に遅れが生じる可能性もあるためだ。また、ランサムウェア攻撃は、制裁を回避し、外貨を稼ぐ手段として使われる可能性についても指摘されている。

昨年五月の米コロニアル・パイプラインへのランサムウェア攻撃では、数日間パイプラインの稼働が停止した。ガソリンスタンド数千ヵ所が燃料不足に陥り、暴力沙汰も発生、アメリカン航空は航路を一時変更せざるを得なくなった。

そのため欧米の金融業界では、昨年からサイバー演習などを通じてサイバー攻撃対策が進められてきた。また、米国の金融業界は、攻撃者視点で脆弱性を洗い出し、防御強化をしている。さらに、サプライチェーン・リスク対応のため、取引先へのサイバーセキュリティ対策強化も求めている。

③報復のエスカレーション

ロシアによるウクライナ軍事侵攻後、複数の民間のハッカー集団がサイバー攻撃の実施について意思を表明した。国際ハッカー集団「アノニマス」は、ロシア政府機関へのDDoS攻撃やロシアのメディアのウェブサイトの改ざんを行ったと主張している。また、ベラルーシの反体制派ハッカー集団「サイバー・パルチザン」は二月二七日、ロシアの軍用列車二本の運行をサイバー攻撃で九〇分間遅らせたと発表した。

ウクライナ国防省とフョードロフ副首相の呼びかけでサイバー義勇兵とIT軍がそれぞれが立ち上がり、ウクライナ国内外からウクライナ人だけでなく、外国人も加わっ

ているという。ハーバード大学のガブリエラ・コールマン教授（人類学）は、「国家が公然と市民や義勇兵に他国へのサイバー攻撃を呼びかけたのは初めてだ」と指摘する。

副首相がつくったウクライナの「IT軍」には、国内外から四〇万人が参加しているとウクライナ政府は主張しているが、裏付けは取れていない。今のところ、比較的烈度の低いDDoS攻撃などの妨害活動に重きを置いているようだが、メンバーの中には鉄道や電力網への攻撃を呼びかけている者たちもいる。

一方、ロシアの情報機関とのつながりが指摘されているランサムウェア攻撃集団「コンティ」は、二月二五日にロシア政府支持を表明しているが、過去に複数の大規模な被害を重要インフラにもたらしてきた。例えば、二一年五月にはアイルランドの国民医療サービスを攻撃し、一部の手術や予約がキャンセルになるなどの被害をもたらした。最終的な復旧費用の総額は、四八〇〇万ドル（五五億円以上）にまで膨れ上がっている。

必ずしも政府の管理の行き届かないさまざまな主体がこれだけ「参戦」すれば、サイバー攻撃を受ける側の政府や軍からすると、誰が攻撃しているのか把握しづらく、事態が混沌としてくる。ロシアがハッカーの身元や攻撃場所を特定したと主張し、そのハッカーが政府と一体となって攻撃していると見なすとすれば、大規模な報復の恐れすらあろう。

リアル世界での戦闘が続き、死傷者が増え、緊張や感情がただでさえ高まっている中、サイバー攻撃の応酬も激化し、事態がどんどんエスカレートしかねない。攻撃元の特定を誤って報復した場合のリスクも懸念される。

米サイバーセキュリティ企業「マンディアント」のジェンズ・モンラッド氏は、サイバー攻撃への参加が、ロシアの侵略や侵攻に対抗するウクライナを支援するための気高い行為と考えることもできると認めつつも、各国の関連法の解釈によっては違法行為となり得ると警鐘を鳴らす。「こうした作戦に参加するもう一つのリスクは、各個人がどれだけ自分の身を守れるか、そして外国人がロシアを標的にしていると把握された場合にロシアがどのように受け止めるかだ」。

「第五の主戦場」になったサイバー空間

サイバー空間が陸、海、空、宇宙に続く第五の作戦領域と目されてから一〇年以上が経つ。今回のウクライナへの軍事侵攻は、サイバー空間も作戦領域の一つとなったこと

サイバー攻撃を行う民間グループ（筆者作成）

ウクライナ側

サイバー義勇兵
- ウクライナ国防省が２月24日に呼びかけ
- ３月４日時点で900～1000人が参加

IT軍
- フョードロフ副首相が２月26日に呼びかけ
- ３月４日時点でテレグラム専用チャンネルに28万5000人参加

サイバー・パルチザン
- ベラルーシの反体制派ハッカー集団
- 2022年１月時点で20～30人

アノニマス
- 国際ハッカー集団

ロシア側

コンティ
- ランサムウェア攻撃集団

ストーモス
- ランサムウェア攻撃集団
- アラビア語を使用

クーミングプロジェクト
- ランサムウェア攻撃集団

レッドバンディッツ
- サイバー犯罪集団

を現実問題として世界に突きつけた。さらに、政府や軍所属ではないハッカー集団が世界各地から「参戦」するという未曾有の事態が出来し、サイバー空間における応酬が複雑化。サイバー攻撃の思わぬ飛び火が懸念されている。

国土に侵略してきた軍が病院や学校をも砲撃し、市民の死傷者が拡大する中、地上戦を戦う義勇兵は許されても、国内外の人々にサイバー義勇兵としてサイバー攻撃の実施を呼びかけるのは許されるのか。その場合、どのようなサイバー攻撃であればよいのか。それとも、あくまでも重要インフラをサイバー攻撃の被害から守るための情報提供や技術支援に徹するべきなのか。

また、義勇兵を装い、私憤を晴らそうとするハッカーや、私腹を肥やすための金銭目的のサイバー攻撃を仕掛けるハッカーをどう見分け、処罰するのか。勤務先に無断でサイバー義勇兵として参加した後、相手国から身元を特定され、勤務先の政府や企業にサイバー攻撃を仕掛けられたならば、本人と相手国にどのように対処すればよいのか。今回のウクライナ侵攻を機に難題が世界に突き付けられている。

新たな国際規範を整理するため、国際的な議論が早急に必要である。日本は、今まで、国連政府専門家会合における国際規範づくりに積極的に関わってきた。国際規範は各

国の国益と思惑が絡み合い、一朝一夕でできるものではない。しかし、少なくとも日本は、今回浮かび上がった新たな問題点を整理し、議論を国際社会に呼びかけるべきである。

こうした国際的議論を進めていくには、サイバー攻撃の手法や対策、攻撃主体に詳しい技術者やインテリジェンスの専門家だけでなく、国際安全保障や外交、語学、国際法・国内法、戦略的コミュニケーション、心理学など多様な分野の専門家の参加が求められよう。世界情勢、歴史的背景などさまざまな要素が加わって、サイバー攻撃が繰り広げられ、異なるサイバー攻撃主体が「参戦」してくるためだ。

「第五の作戦領域」の規範はつくれるか

一方において、コロナ禍でデジタル化が進む中、ITインフラは世界経済や安全保障の要諦となっている。国際的な緊張の高まりの中で、ランサムウェア攻撃やワイパー攻撃が仕掛けられ、部品やサービスの仕入れ先が感染すれば、供給が滞り、工場などの稼働が一時停止することもあり得るのだ。サプライチェーン・リスク対策を強化するには、各社の事業継続計画にサイバー攻撃への対応も含めたシナリオを盛り込まなければならない。

しかし、顧客企業それぞれが仕入れ先に異なる対策を要求すれば、リソースの少ない中小企業が疲弊してしまう。そのため、業界ごとのルールづくりが業界団体と政府の協力のもとで必要だ。

中小企業を含めた業界一丸となってのサプライチェーン・リスク対策は、非常に大切である。米サイバーセキュリティ企業「ファイア・アイ（現マンディアント）」の調べでは、サイバー攻撃の七七％が、サイバーセキュリティ予算や人手のない中小企業を狙っている。企業の自助努力も啓発活動で促しつつ、中小企業が最新のサイバー攻撃の手口に合わせた対策を取れるよう、政府からの情報提供や助成金などの支援も進めていくべきであろう。

戦時におけるサイバー攻撃対処のための国内外の協力のあり方を含め、世界は世紀の難題に直面している。サイバー攻撃を国家戦略として使い続けている国々は、世界がどうこの難局を乗り切るか、固唾をのんで見守っているはずだ。日本も世界も、短期的な個々の組織のサイバーセキュリティ強化、中期的なサプライチェーン対策、そして長期的な国際規範の確立を進めていかなければならない。それが、戦時と平時を含めた日本と世界のサイバーセキュリティ向上につながるのだ。●