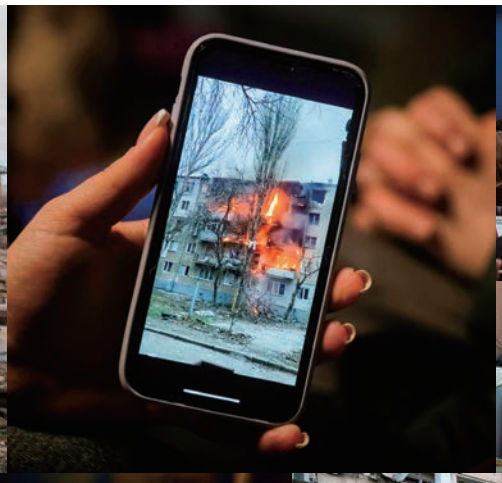
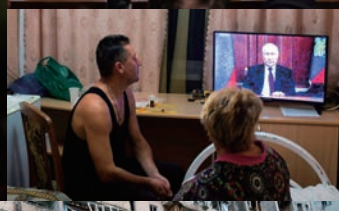
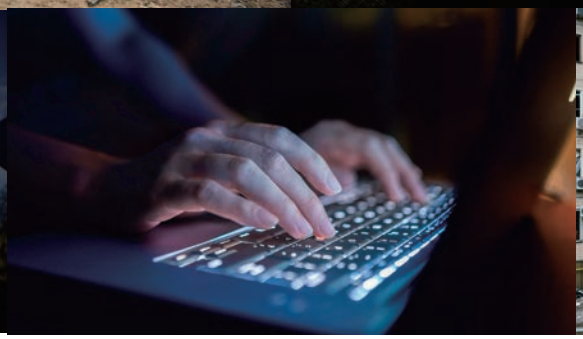
MIT Technology Review
Published by KADOKAWA / ASCII

# War in Ukraine

## インターネット時代の新しい戦争




2022 年 2 月下旬、ロシアによるウクライナ侵攻が始まった。世界に大きな衝撃を与えたこの軍事行動は、これまでの「戦争」の概念を変えるものだ。従来の地上での軍事攻撃に加えて、サイバー空間を狙ったハッカーらによる攻撃も同時に実行されたからだ。新しいハイブリッド戦争の時代における各国の動きと市民らの抗議行動について、MIT テクノロジーレビューの記事から抜粋した。

# CONTENTS

001 ウクライナ「IT 軍」、ボランティア頼みの危うい現実
006 ロシアのインターネット断絶で現実味増す「スプリンターネット」
012 ロシアを標的とした「抗議ウェア」、オープンソース界に衝撃
016 ロシア「報道の壁」に立ち向かう市民、ネット広告も駆使
024 SNS 駆使するネット探偵、ウクライナで民間「オシント」が活躍
030 露 ウクライナ侵攻で広がるデマ、片棒を担がないためには？
038 ロシア、侵攻直前に衛星通信企業へサイバー攻撃 端末数千台破壊
041 サイバー・アトリビューション、露ウクライナ侵攻で重要さ増す
046 転換期を迎えた米サイバーセキュリティ政策、規制強化の舞台裏

Kenny Holston/Getty Images

# ウクライナ「IT 軍」、ボランティア頼みの危うい現実

ロシアと戦うハッカーを募集――ウクライナ政府の行動は意外なものだった。
世界中の志願兵によって構成される「ウクライナ IT 軍」の参加者は攻撃実績を喧伝しているが、
そのほとんどで裏付けは取れていない。プロパガンダ戦争の様相を呈している。

ロシアがウクライナを侵攻したとき、ウクライナ政府はすでに別の反撃方法を考えていた。

2 月 26 日、ウクライナのミハイロ・フョードロフ DX（デジタル・トランスフォーメーション）担当大臣は、「ウクライナ IT 軍」を立ち上げた。ウクライナのためにロシアを攻撃するよう、世界中のハッカーたちに呼びかける前代未聞の試みだ。ウクライナ IT 軍は、さまざまなプレイヤーが入り乱れ、検証不能な破壊工作の主張が飛び交う一方、目に見えるハッキング活動が非常に少ないといった特徴を持つ、今回の複雑なサイバー紛争でもっとも目に付く勢力になっている。

実際のところ、戦争が始まってから 1 週間、ハッキング活動の痕跡はほとんど見られなかった。むしろ、ウクライナ IT 軍をはじめ、サイバー攻撃の意思を表明しているあらゆる集団は、ウクライ

ナとロシアだけでなく、全世界に影響を与えるプロパガンダ戦争に忙しかったのだ。

国際的なハッカー集団に助けを求めるウクライナの戦略は、窮地に追い込まれた国の動きとしては理にかなっていると専門家は指摘する。IT 軍への参加希望者はテレグラム（Telegram）のチャンネルに誘われ、一連のメッセージによって明確な目的が提示される。ハッキングや DDoS（分散型サービス不能）攻撃のターゲットは、ウクライナ陣営のための情報戦を展開する方法を説明する文書と併せてリスト化されている。リストには政府機関や金融機関が含まれており、ロシアの重要なインフラに照準を定めていることが明示されている。テレグラムのチャンネルにはこれまでに 27 万人以上が登録した。

数多くのランサムウェアを操るハッカー集団も、紛争に参加する意向を表明している。ただ、繰り返しになるが、（ハッキングするという）メッセージはすぐに大きく報道されたものの、いずれの集団も目に見える裏付け可能な攻撃を実施していない。アノニマス（Anonymous）などのハクティビスト（政治的な主張のためハッキングをするハッカー）集団は、ロシア政府のデータベースに侵入したと主張するなど、自らの関与を声高に言い立てているが、そうした表明のいくつかはすぐに否定された。しかし、大げさな声明や誤った情報は、野火のようにうまく広がった。詐欺師、嘘つき、ペテン師が戦争の混乱に拍車をかけているのだ。

この混迷は、大物集団や政府によって組織された集団にまで及んでいる。「ベラルーシ・サイバー・パルチザン（Belarus Cyber Partisans）」は、自国内で実際に活動実績がある反体制派のハッキング集団だ。彼らは軍部隊を輸送する鉄道を妨害するため、サイバーインフラと物理的なインフラの双方に攻撃を仕掛けたと主張しているが、その裏付けは取れていない。

ウクライナ国防省関係者によって組織されたウクライナのサイバー・レジスタンス集団は、ロシア国内の鉄道や電力網をターゲットにしていると話している。これも大胆な主張だが、何の証拠もない。専門家は、送電網に影響を与え

られるサイバー攻撃能力を持つ国はごくわずかだと考えている。

ロシアやベラルーシと関係のあるハッキング集団「ゴーストライター（Ghostwriter）」は、ウクライナの政治家や軍人をターゲットにしているのが確認されているが、これまでのところ有意義な成果を上げられていない。サイバーセキュリティ企業イーセット（ESET）のジーン - イアン・ブータン脅威研究部長によると、侵攻の数時間前、ウクライナ政府が掲げたターゲットに対して、未知のハッキング集団が破壊的なワイパー型マルウェアを使用したが、どのような影響を与えたかは不明なままだ。

ロシア国内で実際に何が起きているのか？ 同国最大のサイバーセキュリティ企業であるカルペルスキーの専門家へ取材を申し込んだが、拒否された。だが、何かが起きている。ロシア外務省のマリア・ザハロワ報道官は先日、ロシアのメディアに対し、ロシアは「ウクライナのサイバー・テロリスト」によって攻撃を受けていると語った。

米国のサイバーセキュリティ企業、クラウドストライク（CrowdStrike）のアダム・メイヤーズ部長は、「（サイバー紛争に）これほどまでにさまざまなプレーヤーが登場するのは初めてのことです」と言う。

しかし、ウクライナ各地の都市中心部にいる数百万人もの人々が激しい砲撃を受けているとき、データベースからの情報漏洩や機能不全に陥ったWebサイトの本当の価値とは何なのだろうか？ この国際的な「軍隊」は果たして実際にどれほどの影響を与えたのだろうか？ 何とも言えない。ウクライナIT軍が特定のIPアドレスをリストに掲載すると、そのターゲットがダウンすることはよくある。それも、比較的早いうちにだ。ロシアのサイトの多くは現在、海外からの接続をすべて拒否しており、ロシア国内のみで運営されている。歴史的に前例のない規模の、国際的な攻撃に対する防御のためだ。

DoS攻撃は技術的には単純なもので、復旧は難しくない。都市の中心部を攻撃するロシアのミサイルや、侵攻軍を撃退するウクライナの火炎瓶と比べれば、破壊力ははるかに低い。

これらすべてが、ウクライナとロシア、そして世界で起こっている情報戦争に影響を及ぼす。ロシアが侵攻前に実行したウクライナの政府機関や金融機関へのサイバー攻撃は、ウクライナの指導者に対する信頼失墜を目的としていたようだ。同様に、ウクライナ政府がロシア政府のサイトをダウンさせることは、ロシア国内に対して独自のメッセージを発信しようとする、ウクライナ流の情報戦である。首都をほぼ完全に包囲されたウクライナは、重要な生命線である西側からの支援を受けて、地上とサイバー空間で抵抗を続けている。

「サイバーは、戦争やスパイ活動に活用される武器の1つです」とメイヤーズ部長は言う。「公然と武力紛争が起こっているのです。（ウクライナ政府の世界中のハッカーへの呼びかけは）外国人たちにウクライナに来てカラシニコフ銃を手にして、地上でロシアと戦ってほしいと言っているのと何ら変わりません」。

一方、ワシントンやロンドンにいると、その様相は少し違って見える。欧米の各国政府は長年にわたり、ロシア国内からのサイバー攻撃を非難してきた。ウクライナが公然とハッカーに助けを求めている今、何が起こっているのだろうか。

「米国政府は『ハクティビストが米国のルーターを使って、ロシアのプロパガンダ・サイトに対するDDoS攻撃を仕掛けるのを許可していない』と言っていますが、ロシアはそれを信じないでしょう」。米国中央情報局（CIA）の元ロシア担当分析官、マイケル・E・ヴァン・ランディンガムは言う。「ロシアは国家権力の延長としてサイバーツールを使います。そしてロシアの指導者たちは多くのことを鏡像と捉えます。つまり、アノニマスや西側のハッカー集団からの攻撃を、西側政府が推進する攻撃として認識するでしょう」。

ウクライナIT軍が推進している多くのサイバー攻撃は、米国をはじめとする欧米諸国では明らかに犯罪だ。しかし、この状況は法的な問題だけでなく、新しい道徳的、地政学的な問題を浮き彫りにする。

「西側諸国の政府は、ロシアのサイトを改ざんしたり、DDoS攻撃を仕掛けたり、サイバー空間で何らかの違法行為に手を染めようとしたりす

る者に対して、ハッキングを禁じる法律を厳格に執行すべきです」とヴァン・ランディンガム元分析官は言う。「それが、CIA の陰謀ではなく、米国サイバー軍の攻撃でもないことを示す唯一の方法です。犯人が誰か、私たちが何をしているのかを示すことです」。

混沌とした状況の中、ロシアのウクライナ侵攻と同時に起こった検証不能な大規模サイバー作戦は、戦争全体に立ちはだかる大きな謎の１つとなっている。ロシアは近年、ウクライナに壊滅的なサイバー攻撃を仕掛けてきたが、侵攻以来、伝統的な地上戦に固執している。戦争の長期化に伴い、ロシアが今後数週間から数カ月のうちにサイバー攻撃に転換する可能性があるかどうかが新たな争点になる。（Patrick Howell O'Neill）


Ms Tech

# ロシアのインターネット断絶で現実味増す「スプリンターネット」

世界共通のコミュニケーション基盤である、
単一のグローバル・インターネットの存続が揺らいでいる。
もし、インターネットの分断（スプリンターネット）が起こったら、元に戻すのは難しいだろう。

ロシアが西側諸国のオンライン・サービスから断絶したのは、現実の世界貿易ルートから断絶したのと同様に、突然の出来事であり、完全なものであった。

フェイスブックはロシア当局によって完全にブロックされており、ツイッターもほぼ完全に遮断されている。さらに、アップル、マイクロソフト、ティックトック（TikTok）、ネットフリックスなど、多くの企業がロシア市場から自主的に撤退した。ロシアは急速に、イランのようなデジタル・パーリア国家（日本版注：国際的に孤立した状態にある国家のこと）になりつつある。

一方、欧州連合（EU）は、ロシアの特定のサイトをインターネットから一掃しようとしている。国営放送のRT（旧ロシア・トゥデイ）とスプートニク（Sputnik）に対する新たな禁止措置では、

これらのサイトをブロックするだけでなく、検索エンジンやソーシャルネットワークに対し、上記サイトからのコンテンツを引用する投稿を非表示にするよう求めている。

しかし、これらの断絶されたものはすべて、インターネットを動かすテクノロジーや取り決めというよりもむしろ、インターネットを利用したサービスに過ぎない。フェイスブックがある国でブロックされるということは、基本的に、フェイスブックがある国から撤退したり、あるいは単に倒産したり、閉鎖したりすることと、何ら変わりはない。

しかし、双方の行動によっては、より深刻な分裂が起こる可能性がある。ロシアは、フェイスブック、インスタグラム、およびワッツアップ（Whatsapp）を所有するメタを「過激派組織」であると宣言。さらに、欧州評議会（Council of Europe）などの国際統治機構から脱退し、欧州放送連盟（European Broadcasting Union）からは活動停止処分を受けている。このような動きがインターネットを管理する組織で再現されれば、極めて甚大な影響を及ぼすことになるだろう。

こうした動きにより、「スプリンターネット（日本版注：分断されたネットの意。スプリンター（splinter、破片の意）とインターネットを組み合わせた造語）」、またはバルカン化したインターネット（日本版注：ある地域や国家が互いに対立する地域や国家に分裂していくこと）への懸念が高まっている。すなわち、現在の単一のグローバルなインターネットの代わりに、互いにやり取りすることがなく、おそらく互換性もないテクノロジーを使って動作するネットワークが、多数の国や地域で存在することになるのではないか、という懸念である。

そうなれば、世界共通のコミュニケーション・テクノロジーとしてのインターネットは、終わりを告げることになる。それは一時的なことではないかも知れない。中国やイランは現在、たとえ一部のサービスしか利用できないとしても、米国や欧州と同じインターネット・テクノロジーを使用している。そのような国がもし、競合となるガバナンス組織やネットワークを構築した場合、その

ネットワークを再構築するには、世界中の主要国が相互に合意するしかない。世界がつながっている時代は終わるだろう。

このような動きはすでに出ている。2 月にウクライナ政府は、インターネットのドメイン名システムを管理する ICANN（Internet Corporation for Assigned Names and Numbers）に対し、ロシアの同システムへのアクセスを停止するように要請し、事実上、インターネットから「.ru」サイトを排除しようとした。

ICANN はかつて、米国商務省の外郭団体であったが、現在は非政府組織として運営されており、ウクライナ政府の提案を全面的に拒否した。

ICANN のゴーラン・マービー最高経営責任者（CEO）は、「インターネットは非中央集権型システムです。誰かがそれを制御したり、停止させたりすることはできなません」と、ウクライナの提案に対する回答に記している。「本来、ICANN はインターネットを確実に機能させるために設立されました。調整の役割を利用してインターネットの機能を停止させるためではありません」。

マービー CEO の警告はもっともだ。ICANN は、法制度や法令に基づくドメイン名システムに関する権限を持たない。ICANN の決定はすべてのインターネット事業者が自主的に受け入れているのである。何事も合意形成が必要であるため、意思決定には時間がかかるが、インターネットを維持するには有効である。

インターネットの他の統治機関も、ほとんど同じように機能している。力ではなく合意によって機能する独立した国際機関なのだ。世界の重要なインフラを運用するには、奇妙で不格好な方法であることにほとんどの人が同意しているが、誰もが同意するような良い代替案はない。

インターネットの新しいガバナンスに合意しようとすると、世界各国の合意が必要になる。これは 21 世紀には存在しないほど稀なことである。しかし、そのことはとりもなおさず、インターネットがお互いの自発的な合意によって支えられているに過ぎないことを意味する。

それでは、実際のスプリンターネットはどのようなものなのであろうか。そして現在、それにど

れだけ近づいているのだろうか。

ジョージア工科大学公共政策学部のミルトン・ミューラー教授によれば、インターネットが実際に分裂する場合、同じアーキテクチャー上で別々の国が別々のプラットフォームを使用するのではなく、2つの形態のいずれかになる可能性があると言う。

「インターネットの大規模かつ深刻な分断化には、技術的に互換性のないプロトコルが必要になるでしょう。そのプロトコルを世界中の膨大な数の人々が利用することになります」。

この1つ目のタイプの分断化は、致命的なものにはならないと思われる。「テクノロジストがおそらくすぐに、2つのプロトコルの橋渡しをする方法を見つけるでしょう」とミューラー教授は言う。

2つ目のタイプの分断化は、技術的には互換性のあるプロトコルを使い続けるが、それらのサービスを管理する組織が異なるというものである。 これを元に戻すのは難しいかもしれない。

もしロシアや中国などの国々が、IP アドレスやドメイン名システム（DNS）を管理する現在の団体と競合する団体を設立したとしたら、それは技術的に競合するプロトコルを作った場合以上に、元に戻すのが難しい可能性がある。既得権益が形成され、どちらか一方の側に留まることを望むようになり、再び接続する方針を立てることはほぼ不可能となる。

このような異種ネットワークを単一のグローバルなインターネットに再接続するのは、技術的な問題ではなく政治的な問題である。政治的な問題はしばしば、解決が最も難しい。

また、インターネットが完全に分断化されなくても、世界的な情報の流れが阻害されたり、パーリア国家においてインターネットが適切に機能することを阻害されたりする可能性がある。

インターネットは独占を生む性質があるため、サービスによっては準インフラ的な位置づけになるものもある。例えば、アマゾン Web サービス（Amazon Web Services）は、インターネットのバックエンドの多くを動かしているため、特定の地域からのアクセスを禁止すると大きな問題と

なる。同様に、ギットハブ（Github）リポジトリへのアクセスを遮断すると、少なくとも一時的に多くのサービスが麻痺してしまうだろう。

ロシアは、公式サイトや公共サイトにおけるこのリスクを軽減しようとしており、そのために、データの本国送還、.ru ドメインの使用、海外のサービスプロバイダーの使用を最小化しようとしている。一部の人々はこれをロシアの全 Web サイトに対する指示だと受け止めてパニックが起こり、ロシアがインターネットを完全に遮断することを計画しているとする警告的な記事も出た（ただし、今のところ確証はない）。

インターネットのグローバルな性質を緩和しようとする国や団体は、独裁国家だけではない。欧州連合は、自国民についてのすべてのデータを自国内で処理するよう求めており、米国の大手テクノロジー企業はこれに激しく抵抗している。

一方、イランは主要なオンライン機関同士の国内接続を構築している。グローバルなネットワークから自らを遮断する必要がある場合、あるいは敵対国に追い出された場合、イランだけの機能的なインターネットを運用できるようにしている。

しかし、インターネットと最も複雑な関係にあるのは、おそらく中国であろう。中国発のテック企業は、ティックトックに代表されるようにしばしば西側諸国で成功を収めている。だが、中国国内で人々が利用するオンラインサービスのほとんどは中国企業によるものである。また中国政府は、グレート・ファイアウォールと呼ばれる大規模なオンライン検閲を定期的に実施している。

中国のインターネット検閲を追跡している非営利団体、グレートファイア（GreatFire）のチャーリー・スミス（中国で活動し、検閲政策に批判的であるため仮名）は、中国とグローバル・インターネットとの関係は時代とともに変化してきたと言う。

「当初、サービスレベルのブロッキングは、純粋な検閲の必要性から実施されました。習近平に関する情報を隠したり、政府に直接の責任がある大災害を隠蔽したりする必要があるのです。ですが、海外の Web サイトがブロックされるにつれ、中国の起業家は市場に埋められる隙間があること

に気づきました」とスミスは言う。

「彼らはその隙間を埋めるだけでなく、西側諸国の企業と同じように価値のある、中国のインターネット企業を生み出すことに貢献したのです。たとえこれらの中国企業が中国国外では十分な地位を確立していないとしても、です」。

こうした長年にわたる独立機関のおかげで、中国はインターネットから切り離されても何とかなるとスミスは主張している。だが、そうすることが中国の利益になることはほとんどない。

「中国はグローバルなインターネットから自国を切り離す可能性があると思いますし、国内で十分な危機があれば、おそらくそうするでしょう。しかし中国は、これからもグローバル・インターネットに依存していくと思います。中国のディアスポラ（自国から離れて暮らす集団）は世界のいたるところにいます。誰も家庭とのつながりを切断したくはありませんし、企業は今後も海外で製品を販売することに依存するでしょう」。

グローバルなインターネットから自国を切り離す代わりに中国は、十億人以上のインターネット・ユーザーを抱える国として、インターネットを管理するさまざまな組織の要職に就いている。そして、標準やルールやプロトコルを次第に、自国の都合の良いように曲げようとしている。

テクノロジーよりもむしろ政治によってスプリンターネットが引き起こされる可能性は非常に高い。しかし今のところ、誰もが自分たちに有利になるように、もろい現状を維持して微調整しようと躍起になっているように見える。少なくとも、インターネットの分断化を許してしまえば、修復は不可能になると思われるからだ。（James Ball）


AP

# ロシアを標的とした「抗議ウェア」、オープンソース界に衝撃

ロシアのウクライナ侵攻に抗議する「プロテストウェア」が
オープンソース・ソフトウェアの利用者らに衝撃を与えている。少なくとも 1 つの OSS プロジェクトに、
ロシアとベラルーシにあるコンピューターのファイルを消去することを目的とした
悪意のあるコードが追加されていた。

ロシアのウクライナ侵攻に対する抗議メッセージを表示するよう改変されたオープンソース・ソフトウェア「プロテストウェア（protestware、プロテストは抗議の意味）」の広がりを受けて、ロシア最大の銀行がユーザーにソフトウェアのアップデート中止を呼びかけている。

プロテストウェアのほとんどは反戦や親ウクライナ派のメッセージを表示するだけで、ユーザーに実害はない。ただ、少なくともある 1 つのプロジェクトでは、ロシアやベラルーシにあるコンピューターのファイル消去を目的としたコードがソフトウェアに追加されており、意図しない巻き添え被害に怒りの声も上がっている。

ロシアの銀行最大手であるベルバンクは、リス

クを回避するためソフトウェアのアップデートを一時的に実施しないこと、アップデートが必要なソフトウェアについてはソースコードを手動で確認するよう勧告した。ただ、これはほとんどのユーザーにとって非現実的な対応だ。

ロシアメディアやサイバーセキュリティ企業が報じた声明によると、ベルバンクは、「ユーザーにはソフトウェアのアップデートを今すぐ中止するよう求めるとともに、開発者には外部のソースコードの使用に対する管理を強化するよう求めます」と述べている。

ウクライナ侵攻が始まったとき、ロシアに制裁を加えるため、テック企業はロシアのユーザーに対するソフトウェア・アップデートの提供を取りやめるべきだ、との意見が一部で上がっていた。プロテストウェア運動を追跡している観測筋によると、実際にアップデートの提供をやめたテクノロジー企業はないものの、二十数件のオープンソース・ソフトウェア・プロジェクトで、反戦を訴えるコードの追加が確認されている。オープンソース・ソフトウェアは、誰もが改変や検査ができるソフトウェアだ。透明性が高く、少なくともこの場合は破壊行為に対してもオープンになっていると言える。

## 巻き添え被害?

これまでで最も深刻なプロテストウェアは、「ノード・ドット・IPC（node.ipc）」で発生した。ノード・ドット・IPC は、毎週 100 万回以上ダウンロードされている人気のオープンソース・プロジェクトだ。開発者である RIA エバンジェリスト（RIAEvangelist）は、「ピースノットウォー（PeaceNotWar）」という戦争に抗議するコードを書いていた。ギットハブ上の説明によると、このコードはユーザーのデスクトップに「平和のメッセージ」を追加するものだという。

「このコードは、ノード・モジュールの制御がなぜ重要なのかを示す、非破壊的な例となります」と開発者は記している。「また、たった今世界を脅かしているロシアの侵攻に対する非暴力的な抗議の意味も込められています。（中略）はっきり

言って、これはプロテストウェアです」。

だが、実際のノード・ドット・IPC には、ユーザーの位置を特定し、ロシアやベラルーシ内で実行された場合にコンピューター内のファイルを消去するコードが追加されていた。

サイバーセキュリティ企業、スニーク（Snyk）の研究者であるリラン・タルによると、悪意のあるコードは 3 月 15 日に追加されていた。Base64 でエンコードされたデータ内に隠匿されていたため、発見が難しくなっていたという。

改変されたノード・ドット・IPC がダウンロードされた直後、実際にベラルーシにある米国の NGO によって運営されているサーバーが被害に遭い、「ロシア軍と政府高官によるウクライナでの戦争犯罪を記録した 3 万件以上のメッセージやファイルの消去につながってしまった」との主張がギットハブに投稿された。

スニークの調査によると、このコードがパッケージの一部として残っていたのは一日足らずだという。米国の NGO からとされる前のメッセージは検証されておらず、どの団体からも被害についての公式発表はない。

「抗議が目的とはいえ、今回の問題は、ソフトウェアのサプライチェーンが直面しているより大きな問題を浮き彫りにしています。コード内の推移的な依存関係が、セキュリティに大きな影響を与える可能性があります」とタル研究員は記している。

オープンソース・ソフトウェアの開発者自らがプロジェクトを妨害するのは、今回が初めてではない。今年 1 月には、「カラーズ（colors）」と呼ばれる別の人気プロジェクトの作者が、無限ループを追加してしまい、問題が修正されるまで同ソフトを実行していたすべてのサーバーを使い物にならなくしてしまった。

## 新たな動き

プロテストウェアは、ロシアの検閲を突破して反戦メッセージを届けるために活動家たちが実行した多数の技術的な試みの 1 つだ。活動家たちはターゲット広告を使ってニュースを発信してい

る。ウクライナ侵攻に関するニュースを、加速する検閲と偏在する国家プロパガンダに翻弄されているロシア国民に届けているのだ。クラウドソース化されたレビューの書き込みや反戦のポップアップ・メッセージは、ロシア軍の侵攻が始まって以来採用されている戦術となっている。

プロテストウェアは、ウクライナ周辺で展開されている「サイバー戦争」のうち、目に見えるものの多くが、何よりもまず情報戦とプロパガンダ戦争に直接関係していることをさらに証明するものだ。

プロテストウェアは反戦メッセージを伝えることができるが、オープンソース・コミュニティは、破壊工作の可能性、特に単純な反侵略メッセージを超えてデータを破壊し始めた場合に、オープンソースのエコシステムが損なわれることを懸念している。商用ソフトウェアほど知名度はなくとも、インターネットのあらゆる面を動かすためにオープンソース・ソフトウェアは非常に重要な存在だ。

「パンドラの箱が今開かれました。これからオープンソースを使う人々は、かつてないほどの外国人排斥を経験するようになります。誰もがそこに含まれます」。ギットハブのあるユーザーであるNM17はこう記している。「オープンソースの信頼性は、開発者の善意に基づくものでしたが、今では事実上失われ、今やますます多くの人々が、ある日突然、自分のライブラリーやアプリケーションが、インターネット上の開発者の誰かが『正しい行動だった』と考えたことを実行したり発言するために悪用される可能性があることに気づいています。この『抗議』から何一つ良いことは生まれていません」。（Patrick Howell O'Neill）

AP Photo/Denis Kaminev, File

# ロシア「報道の壁」に立ち向かう市民、ネット広告も駆使

規制強化が進むロシアの報道は日増しに真実から乖離しつつある。
ターゲティング広告やポップアップ通知などのさまざまな手法を駆使して、
市民に正しい情報を提供しようとする試みが広がっている。

ターゲティング広告はインターネットのいたるところで人々に付きまとい、思わず笑ってしまうようなミームTシャツから高級スリッパまで、さまざまな物を売り込んでくる。そして今、トラッキング・ピクセルとポップアップ広告の力を借りて、ロシアの一般市民にウクライナ侵攻の真実を届けようとしている人たちがいる。

「ウクライナで起きていることを伝え、ウクライナの利益を代弁し、国際的な支持を取り付けるために、市民社会が大きな役割を果たすことはすでに知られています」。英国外務省でデジタル外交を担当した経験もある外交交渉の専門家、ジャック・ピアソンは言う。「ロシア政府の情報統制を突破し、一般市民に情報を届けようと、いまや世界中のコミュニティが取り組んでいます」。

現在、信頼できるニュースをロシアで入手する

のは困難だ。国営報道機関は、今回の侵攻は自衛のための措置であると視聴者に伝え、TV レイン（TV Rain）などのロシアの独立系報道機関は当局によって閉鎖に追い込まれた。一方で、BBC やボイス・オブ・アメリカ（Voice of America）などの国際報道機関へのアクセスは遮断されている。情報の空白を埋めるため、少数の活動家はロシアのファイアウォールの穴を利用して、日増しに真実から乖離しつつあるロシアのメディア・エコシステムに、わずかな真実を提供しようとしている。

ロシアのプロパガンダ体制に風穴を空けようと、活動家はあらゆる手段を講じている。ロシアの薬局チェーン、オゼルキ（Ozerki）の利用者は 2 月 28 日夜、ウラジーミル・プーチン大統領の行為に対して「目を覚ます」よう促すスマホのプッシュ通知を受け取った。通知の内容は、プーチン大統領は同胞を戦争に送り込み、ロシア兵士の命のみならず、ロシア国民の財産をも奪おうとしているというものだった。オゼルキはその後のコメントで、同社はハッキングの被害にあったと説明した。さらに別のデジタル・キャンペーン活動家たちは、「ロシアのグーグル」と呼ばれるヤンデックス（Yandex）に、ロシアの主要な施設の偽のレビューを大量に投稿し、プーチン大統領のウクライナ侵攻に関する真実を広めようとしている。ウクライナ出身で米国在住のある学者は、数千人のロシアの同僚にメールを送り、ロシア軍が現在ウクライナで何をしているのかを知らせた。

ベルリンの Web デザイン会社「ニュー・ナウ（New Now）」は、Web ページに埋め込めるスクリプトをギットハブに投稿した。このスクリプトを Web ページに埋め込むと、ロシアの IP アドレスからアクセスした利用者に対して、ロシア政府は嘘をついており、罪のない人々や子どもが殺害されていると伝えるポップアップを表示する。

「開発者の視点でいえば、全体的にとても簡単なアイデアです」。スクリプトを書いたニュー・ナウのカイ・ニコレードズは言う。ニコレードズは、個人的に運営しているプロジェクトの Web サイトへのアクセス元を見て、このアイデアを思い付いたそうだ。「こうしたプロジェクトは、ロ

シアからアクセス遮断されないでしょう。情報の観点からはあまり重要なサイトでないからです。私たちは国際的な報道機関でも何でもありません。ただ皆を楽しませるようなプロジェクトを運営しているだけです」。コンセプトは、何が起こっているのか分からない人々の意識を高め、すでに何が起こっているかを知っている人々には、より深く考えるように促すことだ。「多くのロシア人は、政府の情報はどこか怪しいと感じているはずだと思いました。しかし、ちょっとした後押しが必要な人もいるかもしれません」とニコレードズは言う。「だから草の根運動を始めようと考えました」。

このほか、ロシア政府による作り話に小さな亀裂を入れるための巧妙な仕掛けとして、ウクライナで起きている真実を伝えることを目的としたネット広告などもある。

ロンドン在住のマーケティング・コミュニケーションの専門家であるロブ・ブラッキーは、ウクライナ紛争に関して、ロシア人読者を独立系ロシア語ニュースサイトへと誘導するターゲティング広告を配信するために、クラウドファンディングで資金を集めている。ブラッキーは自身の手法について、「デジタル広告の世界がつい最近まで完全な未開の地だった」という事実を利用していることを認めている。

ブラッキーが最初にこの手法を試したのは2014年、ロシアが今回とは別の虚偽の口実で、クリミアを一方的に併合した時のことだ。ブラッキーは、クリミア最大の都市、セバストポリに住む人々に対してロシアの侵攻に関するニュースを地域ターゲティング広告を使って表示し、最終的に1000人に閲覧された。とても小規模な実験だったが、ロシア政府が仕掛けたフェイクニュースのファイアウォールを突破する方法があることを証明した。

現在ブラッキーは、英国の20人ほどの広告関係の仲間と協力し、2月27日に始めた大規模なキャンペーンを進めている。「基本的なコンセプトは、広告配信システムの抜け穴を見つけてロシア国内に広告を配信し、ウクライナの現状を伝える独立系ニュースサイトに人々を誘導することで

す」とブラッキーは説明する。

ブラッキーのチームは、ロシアの検閲当局や広告配信プラットフォームとのいたちごっこを続けている。ロシア当局は侵攻に関する正確な情報を、プラットフォームは不正確なロシア寄りの筋書きをそれぞれ制限したいと考えており、いずれも特定の情報を規制することに躍起になっているからだ。ブラッキーはどこにどのように広告を配信しているかの説明は避けたが、ある一連の広告が3月3日の夜に配信停止に追い込まれたという。「プラットフォーム対策に関しては、考えられるあらゆる手段を試しているとしか話せません」とブラッキーは言う。彼は本業のバイオテック企業のマーケティングでも、似たような状況に遭遇することがあるという。例えば、ある企業は新型コロナウイルス・ワクチンがパンデミックの突破口になるという前向きなニュースを伝える広告を出したが、反ワクチン派の広告を排除するための検閲に引っかかって削除されてしまった。「ロシアの法律に違反することをいとわず根気よく取り組めば、そうした規制を回避することは経験則上可能です」とブラッキーは言う。

ブラッキーらが手がけるこの広告キャンペーンは、ウクライナ情勢について報道をしている「4つか5つ」の独立系Webサイトの URL を選んでロシア人に送り、それらのサイトに連日訪れてもらうことで、ロシア政府の公式見解に疑問を抱くようになることを期待している。だが、ソーシャルメディアだけがそのような活動の場ではない。「現代社会では広告を表示できる場所は無数にあり、その多くを試しているところです」とブラッキーは説明する。もしモスクワ地下鉄のデジタルサイネージにアクセスする方法があれば、そこでも情報を拡散できるかどうか試してみるつもりだという。「規制をかいくぐろうと、日々悪知恵を働かせている専門家はたくさんいますから」。

ブラッキーが集めた資金はまだ2万4500ドルほどだが、キャンペーンはすでに200万人に届き、4万2000人がサイトへのリンクをクリックをしている。いくつかの重要なキーワードの使用が禁止されたにもかかわらず、3月4日の最初の9時間で10万本回以上の広告が配信された。

ネット広告の特性を使いこなし、ロシア国内の特定のユーザーを狙い撃ちにして侵攻に関する情報を伝えているのは、決してブラッキーだけではない。現在「ウクライナ」に言及する1300本以上の広告が、フェイスブックやインスタグラム上でロシア在住のユーザーをターゲットに表示されている（さらに「ウクライナ」のキリル文字「Украина」を含む広告も1100本流れているが、その多くは猫の画像といった当たり障りのない広告）。フェイスブックはロシア国内で同様のサービスを提供するVK（フコンタクテ）ほどは普及していないが、10人に4人のロシア人がフェイスブックを使い、10人中6人がインスタグラムを使っているとの調査結果もある。

これらの広告の多くはウクライナ・ウォー（Ukraine War）という「ニュース・メディア・サイト」が流している。またセーフ・ウクライナ（Safe Ukraine）という「ソーシャルメディア企業」が運用している広告もある。これらの広告には、捕虜のロシア兵士が故郷の両親に涙ながらに電話する心揺さぶる動画や、ロシア市民に戦争に反対するよう呼びかけるテキストが流れるものなどがある。このプロジェクトは、ウクライナ北西の都市ルーツク出身のボーダナ（33歳）によって運営されている（ボーダナは取材に際し、フルネームの開示を拒否した）。

それ以外に、国際業界団体であるインタラクティブ・アドバタイジング・ビューロー（IAB）のウクライナ支部によって組織されている草の根キャンペーンもある。「ウクライナの実情について、より多くの情報を提供しようとしています。ロシアはとても厳しい情報統制下にあり、独立系メディアもありません」。IABウクライナ支部の最高責任者、アナスタシア・バイダチェンコは言う。

戦争開始からの1週間、ウクライナの広告産業は、主にグーグルの広告ネットワークを利用してキャンペーンを展開してきた。ところが最近、グーグルは、ロシアのメディア規制当局である「連邦通信・情報技術・マスコミ分野監督庁（Roskomnadzor）」から、ロシアでの活動においてはロシア政府が「デマ」と見なす内容を広めないよう要請された。3月4日、グーグルは当局

の要請を受け入れ、一時的にロシアでの広告予約機能を停止した。「状況は刻一刻と変化しています」とグーグルは声明で述べている。

これによって、IAB が支援するグループの計画の一部はとん挫してしまった。だがバイダチェンコ支部長は、ロシア当局が広告規制を始めたことは、IAB のキャンペーンが功を奏している証拠だと主張する。

IAB のキャンペーンでは、大量の個別アカウントがそれぞれ少額の広告料をグーグルに支払い、ロシア兵士の母親が含まれる確率の高い層をターゲットに広告を表示させるというものだった。今後は、ヤンデックスでも同様の活動を目論んでいる。「ヤンデックスの利用は厳しく規制されているため、高いリスクが伴うことは理解しています」とバイダチェンコ支部長は言う。「望みは薄いですが、私たちのメッセージをできるだけ多くの人々に届けるために、試す価値はあると思います」。

バイダチェンコ支部長によれば、ウクライナ陣営による同様の取り組みが、ほかにも複数進行中だ。いずれも、戦争開始から数日以内に個別に設立されたグループによって運営されている。「私たちは、それぞれ異なる独自のメッセージで、ロシアのオーディエンスたちにリーチしようとしています」。

IAB のキャンペーンは寄付や支持者に加えて、民間企業からの資金提供も受けている。これらの企業は、プーチン大統領の軍隊によるウクライナでの蛮行を人々に知らせるために、多額の資金を投入しようとしている。「ウクライナ企業のオーナーたちは、危機に直面していることを理解しています。1 万ドルでも 2 万ドルでも、3 万ドルでも 5 万ドルでも資金を使って、ロシアの人々に情報を届け、伝えようとしているのです」（バイダチェンコ支部長）。

バイダチェンコ支部長は 2 月下旬の 1 週間で、ロシアの人々に対してより信頼性の高い情報を伝えることを目的としたウクライナの広告キャンペーンに、総額で 33 万ドルが費やされたと試算している。そうした広告キャンペーンは、マルタ大学で国家安全保障と諜報活動を研究する博士課

程学生のアグネス・ベネマが「2022 年版の地下新聞」と呼ぶものも含まれる。「人々はプーチンが得意とする手法を、逆手に取ることを覚えたのです。インターネットに接続しているロシア人であれば誰もが閲覧できるような方法で、デマに対抗する情報を流すことができます」。

とはいえ、多額の資金を投入しているにもかかわらず、望まれる効果はないとの懸念もある。「広告は無駄に終わると思います」と語るのは、西イングランド大学でソーシャルメディアと政治について研究しているスティーブン・バックリー特任講師だ。「多くの人は広告ブロッカーを利用していて、この手の広告のクリック率はとても低いからです」。バックリー特任講師は、最も成功しそうなのは、ポップアップで通知を表示させるニコレードズのスクリプトだと考えているが、その気になればロシア政府はブロックできるとも指摘する。もう 1 つは、ロシアのメールアドレスに直接メールを送る方法だ。BBC は 2019 年からダーク Web 上にミラーサイトを運営している。こうしたサイトへのリンクをメールで送るわけだ。ただ、メールもスパム・フィルターによってブロックされてしまう可能性がある。ベネマも、デジタル広告キャンペーンが特効薬となるという幻想は捨てるべきだと警告する。「ロシア政府によるデマはとても根深く浸透しているため、わずか数本の広告でどこまで効果があるのかは分かりません。いろいろな意味で、ロシア人は陰謀論にとらわれてしまっています。陰謀論に一度はまってしまうと、抜け出すのが非常に困難なのは周知のとおりです」。

他方で、たとえどんなに些細なことであっても、行動を起こせば必ず変化につながると確信している人もいる。「こうした人と人とのふれあいは、持続的かつ大規模に展開できれば、大きな効果を発揮できるかもしれません」とピアソンは言う。「しかしながら、ロシアの一般市民に接触することは、1 つの課題にすぎません。ロシアで反対意見を表明するコストは高く、日増しに高くなっているのです」。

さまざまな活動に取り組む関係者にとって、何もしないという選択肢は最初からなかった。「私

はすぐに、ネット上で何らかの運動を起こす方法はあるだろうかと考えました」とニコレードズは言う。「今の自分ができることは何だろうか。たとえほんのわずかでも、自分が貢献できることは何だろうか。そう考えました。確かに、大海の一滴に過ぎないかもしれません。でも、最後にはその一滴、一滴が大切なのです」。（Chris Stokel-Walker）

Sean Gallup/Getty Images

# SNS 駆使するネット探偵、ウクライナで民間「オシント」が活躍

戦争が始まって以来、世界中の人々が、難民やウクライナの大義を支援しようと動いている。
証拠の収集は簡単な作業に思えるが、その道のりは長い。

2 月下旬、ロシアがウクライナに侵攻した時、エイデンは多くの人と同じように無力感を感じていた。エイデンは英国在住の 23 歳。ウクライナとの繋がりはなかったが、Web 上に公開されているデータを集める「オシント（OSINT：オープンソース・インテリジェンス）」の能力に長けていた。

そこでエイデンは、調査団体ベリングキャット（Bellingcat）のボランティアとして参加し、ウクライナで起きている戦争犯罪の可能性がある活動を収めた画像や映像の確認作業を手伝うことにした。ベリングキャットの活動は、最終的に国際刑事裁判所（ICC）による訴追につながっていくことが期待されている。

「加害者の行動の責任を追求したいなら、まずその土台となる下準備をしっかりやる必要があります。私たちは今まさにその作業をしています」。エイデン（本人の希望により名字は伏せている）

はこう話す。

戦争が始まって以来、世界中の人々が、難民やウクライナの大義を支援しようと動いている。過去にもベリングキャットにボランティアとして参加した経験を持つエイデンのように調査スキルを持つ者にとっての支援とは、時間と労力をかけて、ウクライナ市民がWeb上に投稿した資料1つ1つを分析することだ。彼らは民間施設や病院などの保護区域への爆撃といった戦争犯罪の可能性がある活動を記録し、その正確な場所を確認していく。

2021年1月6日に起きた米国議会での暴動と、それに続くネット上での犯人捜しで培われたスキルは、ウクライナでの戦争におけるネット上での情報収集にも活かされている。ただ、こうした取り組みが潜在的な戦争犯罪の訴追につながる有効な証拠になり得るのか、どのようにしたら証拠として認められるのかは不透明だ。大量に押し寄せる証拠を分類する世界共通のシステムがなければなおさらである。

人権団体は戦争犯罪の可能性を示すデータ収集のため、すでに専門の調査員をウクライナに派遣している。2月23日にキーウ（キエフ）入りしたヒューマン・ライツ・ウォッチ（Human Rights Watch）のリッチ・ウィアー研究員は、翌朝、侵攻のニュースで目を覚ました。

「キーウで同僚が合流する予定でしたが、空域が封鎖されました」。移動先のリヴィウからウィアーはそう教えてくれた。「私は1人ぼっちでした」。

戦争が始まってから最初の数日間、ウィアー研究員は波乱の中で仕事をこなしていった。地元住民から空爆や攻撃について話を聞き、現場に足を運んで被害状況や民間人の死傷者を調査した。

噂やデマが飛び交う情報戦では、検証が重要な鍵となる。攻撃の映像や遺体の写真を見るだけでは不十分な上、ウクライナ国内ではインターネット回線が使用できなくなっている地域も多いため、ウィアー研究員は現場に足を運んだり、避難当事者に話を聞いたりと、アナログな方法で事件を確認する必要があった。

シリアとミャンマーでも同様の仕事をしてきたウィアー研究員によると、紛争が起きるたびにアーカイブ作業は洗練されてきているという。そ

の要因は、ソーシャルメディアやカメラ付き携帯電話の普及にあるとウィアー研究員は言う。

「シリアは潜在的な虐待や人権侵害、国際法に違反する可能性がある行為に関する写真や映像が殺到した、非常に良い例です」。ウィアー研究員は言う。しかしそういったデータがありながらも司法の動きは鈍く、今までのところシリアの独裁者バッシャール・アル＝アサドに対して国際司法機関による訴追はされていない。

それが今回の戦争におけるリスクだ。仮にこの戦争が明日終わったとしても、ウラジーミル・プーチン大統領や戦争犯罪に加担したロシアの司令官たちの刑事訴追が実現するかどうかは不明な上、もし実現したとしても何年もかかるだろう。立件には捜査官らによる位置情報の特定やあらゆるデジタル証拠の確認が必要となる。

このタイムラインを短縮できるのが、そうした作業に取り組む意志と能力を持つ世界中の人々の存在だ。2021年1月6日に米国で起きた議会襲撃事件を記録した経験もここで活きてくるだろう。

「前例となった2021年1月6日の暴動以降、プロセスを合理化してきました」。ベリングキャットのジャンカルロ・フィオレッラ調査員はそう話す。「大量のデータが発生した暴動から得た教訓が役に立っています。戦争犯罪の可能性を示すデータや証拠をより高い割合で集めることができています」。それはエイデンのようなボランティアたちの貢献によるところが大きい。

エイデンは、ウクライナにおける民間人の犠牲や民間インフラの被害に関する証拠の位置情報特定に時間を費やしてきた。自分に割り当てられたインターネット上の写真や映像を、衛星画像やグーグル・マップのストリートビューなどのツールを使って位置を確認している。特定した場所についてエイデンともう1人のボランティアの意見が一致したら（エイデンによると、他の誰かと一緒に証拠を確認することは、視野狭窄を避けるのに役立つという）、ベリングキャットの調査員が独自に情報を検証する。そしてまた最初からこのサイクルを繰り返すという流れだ。

すばらしい取り組みだが、カリフォルニア大学


バークレー校（UC バークレー）人権センターのリンジー・フリーマン法・政策部長によると、こうした取り組みの数の多さや多様性が課題を生んでいるという。善意の取り組みであっても、中には戦争犯罪の訴追に必要な立証責任には単純に満たないものもあるかもしれない。

意外なことに、潜在的な戦争犯罪の刑事訴追につなげるための、紛争地域のデータを正しく収集、保管、提示するルールをまとめた団体や文書は1つもなかった。国連やICCといった国際機関、数多くの人権支援団体など、それぞれ持っている権限や管轄権がバラバラに存在しているためだ。戦争犯罪人たちは真に正義に直面することはないと知っており、彼らの思うつぼになっている。

2020年、フリーマンはオシントの倫理的利用を成文化する取り組み、「バークレー・プロトコル（Berkeley Protocol,）」の立ち上げを支援した。これは国連が支援するプロトコルであり、デジタルデータの取り扱いと記録方法を記したルールブックを提供している。文書の作成にあたっては、シリアから多くの情報を得たとフリーマンは語る。また、フォーマットが混在したことでデータ収集が非常に難しくなるという事実もあった。

このプロトコルはウクライナから洪水のように流れてくるデータを取り扱うためのシステム作りへの第1歩だが、それでは不十分だということを

2022 年 3 月 5 日、ウクライナのマルハリブカ村にて、砲撃を受けた区域を見つめる地元住民。地域警察によると、キーウ南西部にあるマルハリブカ村では、ロシアの空爆により子どもを含む 6 人が死亡、4 人が負傷したという

フリーマンは認めている。多くの支援団体がこのプロトコルを採用している一方で、独自のやり方を維持し、情報を記録するための内部システムを自前で持っている団体も多い。

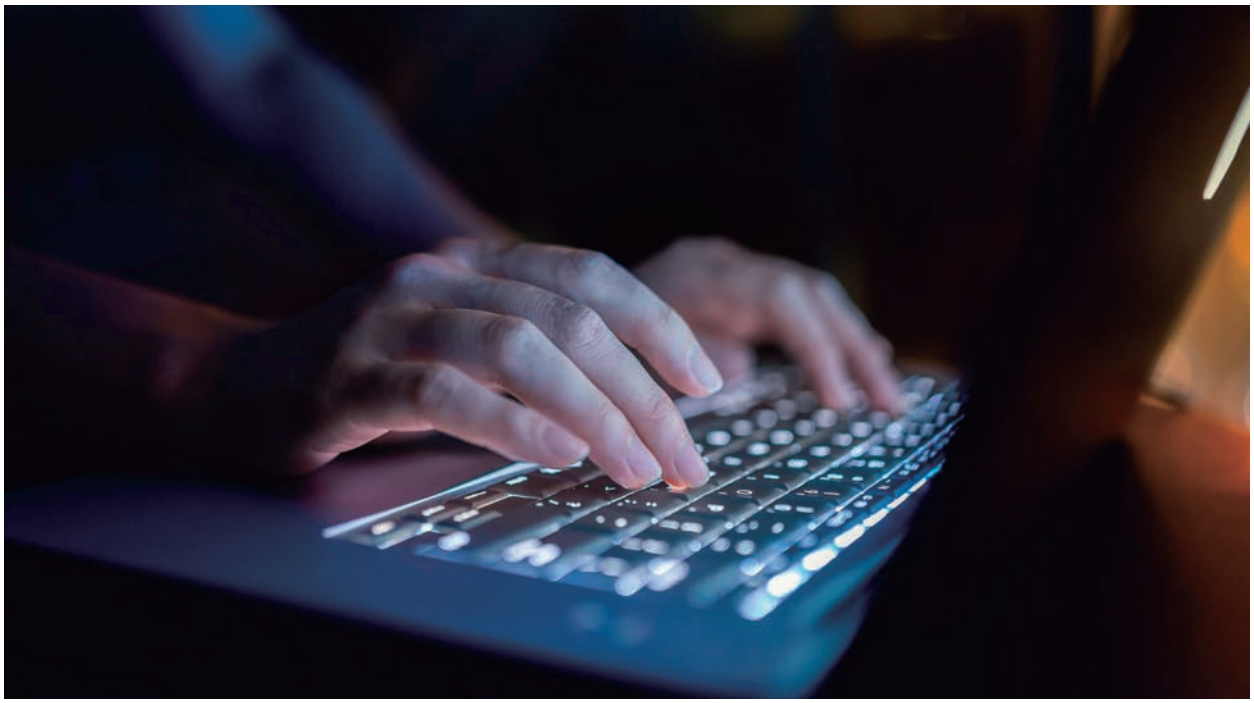
フリーマンによると、バークレー・プロトコルは「クラウド・ソーシングにもあまり対応できていない」という。クラウド・ソーシングはウクライナの戦争のみならず、長年にわたって他の紛争においても重要な要素となってきた。市民がテクノロジーやソーシャルメディアにアクセスしやすくなったことで、被害を受けた人々から権力を持っている組織に直接情報を届けることがかつてないほど容易になったが、このプロトコルではその情報を適切に文書化する方法については言及を避けている。

その理由の 1 つには、ICC が証拠として認める種類を厳しく選別しており、手ブレが大きく画質も悪い携帯カメラの映像よりも、タイムスタンプ入りの監視カメラのような正式な情報源を優先しがちだということがある。

バークレー・プロトコルによって浮き彫りになったのは、ICC が何を証拠として認めるのかということ、証拠を集めようとするクラウド・ソーシングでの取り組みの間の綱引きだ。バークレー・

プロトコルは戦争犯罪人を訴追するためのより確実な足場作りへの大きな第一歩であると同時に、戦争被害者および外部から目を向ける人々、両者のテクノロジーの活用の仕方からICCがいかに圧倒的な後れを取っているかを認識させるものでもある（ICCに繰り返しコメントを求めたが返答はなかった）。

こうした状況でも、エイデンに取り組みを止める気はない。「紛争の被害者にとって、この仕事が影響力を発揮するタイミングはあまりにも遅すぎるのではないかと不安になることもありますが、さかのぼって達成される正義は何も起きないよりはるかにマシだと信じています」（Tanya Basu）



Getty

# 露 ウクライナ侵攻で広がるデマ、片棒を担がないためには？

ロシアのウクライナ侵攻に伴い、ソーシャルメディア上では真偽不明の大量のニュースが飛び交っている。
不用意な情報の拡散はたとえ善意であっても被害をもたらす可能性がある。

2 月 23 日にロシアがウクライナへ侵攻したことを受け、ネット上では次々と情報が伝えられている。写真や映像をはじめとする情報が、真偽の確認ができないほどの猛烈なペースで、各プラットフォームに投稿され、それらが再共有されているのだ。このような現象は、世界各地で何らかの危機が発生するたびに、最近ますます見られるようになっている。

その結果、誤った情報が真実であるかのように受け止められ、増幅されてしまう。善意の人々がそれに加担してしまうこともある。悪意ある行為者たちは、こうした状況を利用して、罪のない民間人に恐怖を味わわせたり、不穏なイデオロギーを広めたりするかもしれない。そうなれば、実際に苦しむ人が出てしまう。

ウクライナ侵攻の正当化を試みてきたロシア政府にとっては、偽情報の流布はその大きな手段となり、あからさまな形で実行されている。ロシア

は、親ロシアの分離派が多いウクライナ南東のドンバス地域で、ウクライナ軍が激しい攻撃を計画し、分離派を標的とした砲撃や大量虐殺をしていると主張した。この主張は誤りだ。でっち上げられた攻撃のフェイク映像は、ロシア国内のプロパガンダ作戦で大きく取り上げられている（これを受けて米国政府は、こうした嘘を暴き、先手を打ってそもそも嘘を流布できない状況にしようと取り組んでいる）。

しかし、政府による活動に関わっていない一般人であっても、今回の侵攻に関して不正確な情報、誤解を招く情報、または誤った情報を意図的に共有してしまう可能性がある。イデオロギー上のナラティブを主張しようと、もしくは閲覧数を上げようとして共有するのだ。しかし、共有したことでどのような悪影響があるのかまではほとんど考えていない。戦争という混乱した状況の中では、意図せず誤って伝えられてしまった情報が、正しい情報として一気に拡散される場合もある。

すでに、ロシアによる侵攻に関する不正確な情報が、ソーシャルメディア・プラットフォーム上で多くの人々の目に触れる状況になってしまっている。ソーシャルメディア・プラットフォームは根本的に、エンゲージメント（いいね！やシェア）を得られるコンテンツを、多くの人に表示するよう設計されているのだ。

ティックトック（TikTok）では、訓練の模様を収めた 2016 年の映像が、あたかも現在ロシア兵がウクライナにパラシュートで降下しているかのような誤った印象を与える目的で共有された。再生回数は数百万回にも達した。ある声明は誤訳された状態でツイッターで大きく拡散され、複数のジャーナリストが共有してしまった。これによって、チェルノブイリ周辺での戦闘で原子力廃棄物貯蔵施設に被害が生じたという誤った情報が広がってしまった（本来の声明は、戦闘によって原子力廃棄物に被害が生じる可能性があると警告する内容だった）。

悲惨な出来事に関してニュース速報が次々と舞い込んできたり、拡散されたりしている。こうした投稿を目の当たりにした人々はしばしば、有害なプロパガンダおよび偽情報をそうとは知らずに

増幅してしまう。意図せず悪意ある行為者たちの手助けをしてしまう状況を避けたければ、本記事を参考にしてほしい。

MIT テクノロジーレビューではこれまでも、ここに挙げたようなアドバイスをいくつか掲載してきた。具体的には、2020 年のブラック・ライヴズ・マターの抗議活動の際、そして同年秋の米国の大統領選挙前だ。以下は、ウクライナからのニュースを扱うにあたって具体的に気をつけなければならない点を反映し、以前に掲載したアドバイスを更新および補足したものだ。

## 重要なのは、1 人 1 人が注意力を発揮すること

まず、1 人 1 人のネット上での行動が大きな影響を持ってしまうことをしっかりと理解してほしい。「自分はインフルエンサーではないから、自分は政治家ではないから、自分はジャーナリストではないからと、自分の（ネット上での）行動はたいしたことがないと人々は考えがちです」と、シラキュース大学でコミュニケーションと修辞学を研究するホイットニー・フィリップス助教授は 2020 年に語っている。しかし、1 人 1 人の行動は、実は重要なのだ。疑わしい情報を共有してしまうと、たとえ共有相手がわずか数人の友達や家族であったとしても、その情報がさらに拡散される原因につながる可能性がある。

## 怒りに任せた引用ツイートや返信に気をつけよう

緊急ニュースになるような事態が発生すると、人々は、良心からそれに異を唱えて批判しようと、ソーシャルメディアの投稿を引用したり、ツイートしたり、共有したり、返信したりすることがある。ツイッターとフェイスブックは、偽情報の流布と戦うために、新たなルール、モデレーション戦略、そして事実確認に関する規定を導入した。しかし、どのような形であれ、人々が偽情報に対して反応してしまうと、拡散を防ぎたいコンテンツを逆に増幅させてしまう危険がある。なぜなら、

反応を起こすことで、プラットフォームに対してそのコンテンツに関心を持ったというシグナルを与えてしまうからだ。不正確であると分かっている投稿があれば、それに反応するのではなく、フラグを立てて投稿先のプラットフォームが審査できるようにしてみよう。

## 一旦立ち止まろう

デジタルリテラシーの専門家であるマイク・コールフィールドは、ネット上の情報の真偽を確認する方法として、「シフト（SIFT、「ふるい」という意味）」を提唱している。これは、「Stop（一旦立ち止まって考えよう）、Investigate the source（ソースを調査しよう）、Find better coverage（よりよい報道を見つけよう）、Trace claims, quotes, and media to the original context（主張、引用、およびメディアファイルをオリジナルの文脈までたどろう）」の頭文字をつなげたものだ。コールフィールドは、ウクライナのニュースに関しては、「Stop」に重点を置くべきだと言う。つまり、表示された投稿に反応したり投稿を共有したりする前に、立ち止まって考えようということだ。

コールフィールドは、「周囲の人々に対して真っ先に自分がその話を共有することで、自分がそのニュースを教えてあげたことにしたいという衝動に駆られるのは、人間なら仕方がないことです」と言う。ジャーナリストは日々、その衝動に気をつけている。しかし、これは誰しもが気をつけなければならないポイントだ。現在のように、情報が次々と舞い込んでくる状況であれば、なおさらだ。

デジタルアナリストでデマを研究しているシャイリーン・ミッチェルは、ウクライナに関するニュースに触れて何らかの行動をしたいのであれば、「自分たちの身に起こっていることについて、ウクライナ現地から伝えてくれる人々をフォローするべきです」と言う。

しかし、ウクライナ発に見える情報だからといって、むやみにリツイートしてはならない。身元がはっきりしている本物のアカウントからの情報だけを共有しよう。ジャーナリストたちは、ロ


シア軍の動きが写っていると思われるティックトック動画の真偽の検証をし、自身の身に起こっていることをウクライナから伝えているように思われる人物からのツイートを共有している。

それでも、細心の注意が必要だと専門家は言う。デマを研究するケイト・スターバードは、ツイッターに優れたスレッドを投稿し、今回の侵攻に関するソーシャルメディアの投稿をいかに精査すべきかを指南している。その中でスターバードは、現在の状況下では、信頼できる周囲の人々でさえ「大急ぎのため、もしかするとそれほどきちんとは精査ができていない」可能性があると指摘している。

スターバードは、偽物かもしれないアカウントを見抜くためのいくつかのポイントを紹介している。

## 自分にできる役割をこなそう

この記事をお読みの方は、おそらくニュース速報記者でなければ、ウクライナとロシアの関係の専門家でもないだろう。専門家は、今このタイミングで専門家ではない人が専門家のように振る舞おうとして、ネット上で見つけた情報の真偽を自分で判断して拡散するのは避けるべきだと指摘する。自身が見かけた情報の真偽を確認しようとするのは常に良いことだが、新たな情報や説を実際に周囲の人々に対して共有するかどうかは慎重に考えてほしい。

ミッチェルは、インターネット上で「人々は自分で調べられるようになったと考えがちです」と言う。ソーシャルメディアでデマやその他の不正

確な情報が拡散されている事実が注目されることで、人々はますますこう思ってしまう。「調べる力が少しはついたと考えているので、今回の動きでも自分で調べられるはずだと考えてしまうのです」。こうした考えは必ずしも正しいわけではない。さらに、悪意ある行為者たちはこれまでも、「自分で調べたい」という衝動につけ込んできた前例が多く判明している。この衝動につけ込んで、蜘蛛の巣のように張り巡らせたデマに人々をおびき寄せようとしてきたのだ。

## あなたにできる最善のことは、足場となる現実をしっかりと把握することだ。

コールフィールドは、英語話者がウクライナからのニュースをリアルタイムで事実確認しようとする場合、「正直なところ、言葉の壁は大きな問題です」と言う。「映像の場所がどこかもわからず、喋っている言語が理解できない状態」なら、その映像を慎重に調べても何が本当かはわかるはずがないと語る。

共有する前に、自分自身に問いかけてみてほしい。話されている言語を自分で翻訳できるか？ それまでに触れたことのないソースからの映像および写真について、調査や分析をするだけのスキルがあるか？ 市民によるジャーナリズムはしばしば非常に深い価値を持つが、正しく実行するには相当のスキルとトレーニングが必要だ。自分には何ができるのか？ なぜ自分にはそれができると言えるのか？ 現実的に考えてみよう。

誤った話を拡散してしまうと、実際に悪影響を及ぼすという事実を、いま一度肝に銘じよう。現在進行中の状況に関して、誤った情報や誤解を招く情報を共有してしまうと、人々を傷けたり死に追い込んだりする原因になる可能性がある。

## その代わりに、正確な情報を拡散して、信頼できるソースからの情報を増幅しよう

このような状況下では、自分の正気を保つためにも、インターネットで自分の情報に耳を傾ける人々のためにも、足場となる現実をしっかりと把

握することが大切な対策だ。英語で信頼できる報道をしているのはどのソースだろうか。誰をフォローして拡散を手助けすれば、正確な情報を広められるだろうか。

自身もウクライナ人で、誤情報に関する報道に携わった経験もあるジェーン・リトビネンコのようなジャーナリストは、ウクライナの慈善活動やニュースメディアを支援したい人向けにまとめた情報を共有し、今回の侵攻を正しく捉えるために欠かせない背景情報も発信している。その他のジャーナリストの間でも、避けるべきプロパガンダまみれのニュースメディアおよびソーシャルメディアのアカウントを、クラウドソーシングで一覧化する動きが出ている。ベリングキャット（Bellingcat）のサイトでは、虚偽であることが判明した主張をスプレッドシートで公開して随時更新している。現地ニュースメディアのキーウ（キエフ）・インディペンデント（Kyiv Independent）は、ツイッターでコンスタントに最新情報を配信している。

コールフィールドは、「あなたの役割は、ニュース記者よりも先に友だちにニュースを伝えることではないかもしれません」と言う。真っ先にニュースを伝えるのは、その道の大勢のプロのすべき仕事だ。「この状況における一般の人の役割とは、事態を説明してくれる信頼の置ける情報源を見つけたり、ロシアが 2014 年にクリミアでいかに偽情報を流したかに関する背景情報を人々に伝えることなのかもしれません」。

## 不正確なことを伝えてしまったら、きちんと訂正しよう

偽情報を見分ける専門家であっても、偽情報を共有してしまう可能性はある。自分がどのような立場にあり、どの規模のプラットフォームに共有するかに関係なく、現在進行形の状況に関して情報を共有するのなら、間違っていた場合には責任を取って訂正し、その影響と向き合う準備をしておかなければならない。

ミッチェルもコールフィールドも、この点に関しては似たようなベスト・プラクティスを推

奨している。ツイッターで不正確な情報を共有してしまったら、不正確なツイートのスクリーンショットを撮り、不正確な情報への返信または引用ツイートという形で訂正を投稿し、その後、偽情報を含むツイートを削除するという手順だ。

ティックトックの場合は仕組みが異なるが、考え方は同様だ。偽情報を削除し、どうしてその映像が削除されたのかを述べ、修正したものを投稿し、フォロワーに対して修正後の情報を共有するよう促すという手順だ。

ミッチェルは、誰であれ、自分が不正確な情報を共有してしまった場合には、その情報を再共有した人々に連絡を取って訂正するくらいの対応をして、その責任を取る準備をしておくべきだと付け加える。

## ログオフも考えてみよう

世界が一大事で、悲惨なことが起きている場合、目を背けたり沈黙したりすると、非情な人間になったように感じられてしまうこともある。しかしそれは違う。ひたすらスクロールして悲観的な情報を読み続ける行為（ドゥーム・スクローリング）はやめよう。（Abby Ohlheiser）

PIERRE CROM/GETTY IMAGES

# ロシア、侵攻直前に衛星通信企業へサイバー攻撃　端末数千台破壊

ウクライナ侵略の直前に米国の衛星通信企業ビアサットがハッキングされ、通信停止に追い込まれていた。地上の軍事作戦と連動したサイバー作戦は、現代の戦争におけるサイバー攻撃の新たな役割を示している。

ロシア軍によるウクライナ侵攻のわずか1時間前、米国の衛星通信企業ビアサット（Viasat）がロシア政府系ハッカーによるハッキング被害を受けていたことが分かった。米国、欧州連合（EU）および英国当局が5月10日に発表した。

このサイバー攻撃の結果、指揮命令系統をビアサットのサービスに依存していたウクライナ軍は当初、重大な通信手段を瞬時に失った。

サイバーセキュリティ企業センチネルワン（SentinelOne）のフアン・アンドレス・ゲレーロ - サーデ主席研究員は、ビアサットへの攻撃は今回の戦争で確認されているサイバー攻撃の中で最も重要なものだと指摘する。「ウクライナの軍事力の無効化を狙った最も組織的な試みだからです」。また、地上の軍事力を強化するために、敵軍が使用するテクノロジーを無力化し、さらには

破壊するサイバー攻撃を適切な標的とタイミングで実施する方法を示した最初の実例でもある。

攻撃は 2 月 24 日に実行された。ビアサットのモデムとルーターに対して、「アシッドレイン（AcidRain）」と呼ばれる破壊力の強いワイパー型マルウェアを感染させ、システム上のデータをすべて即座に削除した。その後マシンを再起動させ、完全に使用不能にした。こうして数千台の端末が事実上破壊されたのだ。

アシッドレイン研究の最前線にいるゲレーロ - サーデ主席研究員によると、かつてロシアが使用していたマルウェアは標的を絞ったものだったが、アシッドレインはより汎用性の高い武器だという。

「アシッドレインの大きな問題は、（攻撃による損害に対する）安全性への配慮が一切ないことです。ロシアの以前のワイパー型マルウェアは、特定のデバイスでのみで実行するように配慮されていました。アシッドレインにはそうした配慮はなく、ブルートフォース（総当たり攻撃）でした。攻撃者は再利用できる能力を手に入れたわけです。問題は、次にどのようなサプライチェーン攻撃が起こるのかということです」。

専門家によると、今回の攻撃は、ロシアが採用した「ハイブリッド」戦争戦略の典型だという。サイバー攻撃が地上の侵攻作戦と連動して進められたからだ。マイクロソフトの研究によれば、このようなロシアのサイバー作戦と軍の正確な連動は少なくとも 6 回確認されており、現代の戦争におけるサイバーの新たな役割が浮き彫りになっている。

「サイバー攻撃の脅威と結果は常に目に見える形で現れるとは限りません。しかし、現代の戦争においてサイバー攻撃が積極的かつ戦略的に使われていることは、ウクライナ侵攻前のロシアの組織的で破壊力の強いサイバー攻撃によって示されています」。デンマークのモルテン・ブスコフ国防相は声明の中で述べた。「サイバー攻撃の脅威は、絶え間なく進化しています。サイバー攻撃は重要なインフラに深刻なダメージを与え、致命的な結果をもたらす可能性があります」。

今回の攻撃による被害はウクライナから飛び火

し、中央ヨーロッパの数千人のインターネット・ユーザーやインターネットに接続された風力発電所に影響を及ぼした。その結果は見かけよりもずっと重大だ。ビアサットは米軍や世界各地の同盟国と協働しているからだ。

「明らかに、ロシアはそうした協力関係を破壊しました」。ゲレーロ - サーデ主席研究員は言う。「ロシアは、これほど被害を広げて EU まで巻き込む意図はなかったと思います。ドイツの風力発電機 5800 基をはじめとする EU 域内に影響を及ぼし、EU に反撃する口実を与えてしまいました」。

アシッドレインがビアサットに対する破壊的な攻撃を開始するわずか数時間前に、ロシアのハッカーはウクライナ政府のコンピューターを「ハーメチックワイパー（HermeticWiper）」と呼ばれる別のワイパーを使って攻撃した。シナリオは不気味なほど似ている。違うのは標的が衛星通信ではなく、ウクライナ政府が侵攻当初に抵抗を開始するのに必要不可欠だったネットワーク上のウィンドウズ・マシンが狙われたことだ。

これらの攻撃がどれほど効果があったのかは、まだはっきりとしていない。ウクライナ政府高官は、ビアサットへの攻撃は「戦争が始まった当初の通信に大損害をもたらしました」と述べたが、詳細は明らかにしていない。

サイバー攻撃が軍事作戦を支えているのは事実だが、今回の戦争で展開されたすべての作戦の全貌が明らかになるには、まだ時間がかかりそうだ。ただし、アシッドレインの仕組みから、再び使われる可能性が高いことは間違いないだろう。（Patrick Howell O'Neill）


AP

# サイバー・アトリビューション、露ウクライナ侵攻で重要さ増す

ホワイトハウスは、ロシアがウクライナに対してサイバー攻撃を仕掛けたとしてすばやく非難した。
効果的な先制攻撃の重要な武器として、サイバー・アトリビューションを位置付けていることを示している。

2 月 15 日から 16 日にかけて仕掛けられた一連のサイバー攻撃の影響で、ウクライナの銀行と政府の Web サイトが一時アクセスできなくなってからわずか 48 時間後、米国はこれをロシアのスパイによる攻撃だと公然と非難した。

ホワイトハウスの国家安全保障副顧問で、サイバー・新興技術を担当しているアン・ノイバーガーは、ウクライナの Web サイトに過負荷を与えて破壊した今回の DDoS（分散型サービス不能）攻撃と「ロシア連邦軍参謀本部情報総局（GRU）の関連を示す技術情報」を米国は握っていると述べた。

ノイバーガー副顧問は 2 月 18 日、「GRU のインフラから、ウクライナの IP アドレスとドメインに対して、大量の通信が送られていたことが観測されました」と報道陣に説明した。今回のサイバー攻撃は、15 万人のロシア兵がウクライナと

の国境付近に集結する中、ウクライナにパニックの種を蒔く意図があったとみられている。

米国と英国の政府関係者が共同で本件をすばやく公表するに至ったことは、これまでに比べて大きな変化であり、米国にとってアトリビューション（属性や帰因の特定）がサイバー紛争においていかに重要なツールになっているかを示すものだ。近年の米国は、サイバー・アトリビューション（サイバー攻撃者を特定し、手法や目的を明らかにすること）を世界のどの国よりも頻繁に地政学的ツールとして利用しており、多くの場合、特に今回のケースのようにターゲットがロシアの場合は英国を同盟国として運用してきた。

「我々がアトリビューションに至るまでのスピードは、異例の速さだったと申し上げておきます」とノイバーガー副顧問は話した。「なぜなら、国家が破壊や動揺をもたらすサイバー攻撃を実行した場合、その責任を負わせる一環として、その行為を迅速に非難する必要があるからです」。

この新しい政策は、2016 年の米国大統領選挙での出来事がベースになっている。米国国家安全保障会議の元局長で、ロシアを担当していたギャヴィン・ワイルドは、米国の大統領選への介入を目的としたロシア政府によるハッキング／デマキャンペーンの内容を詳細に記した画期的なインテリジェンス・コミュニティ・アセスメント（各政府情報機関が参加する組織による評価）の作成に関わった。関連する米国のすべての情報機関を一堂に集め、広範囲にわたる機密レベルの情報を共有するプロセスの始動には、当時のオバマ大統領自らが旗を振り、ジェームズ・クラッパー国家情報長官が後押しするといった多大な努力が必要だった。

だが、ロシアによるサイバー活動の評価とアトリビューションは、米国の大統領選終了後から数カ月後となる 2017 年になるまで公表されなかった。ワイルド元局長は、「ロシアが標的にしていたのは明らかに米国民でしたが、米国の情報機関は（何もできなかったことに）無力感を感じていました」と MIT テクノロジーレビューに語っている。

ただ、公表が遅くなったとはいえ、このアセス

メントはそれまでの何よりも優れた成果となった。

「それでも、ロシアによる作り話が浸透し、著名人たちがそれを増幅する前に、そうした活動を沈静化できなかったという挫折感がありました」とワイルド元局長は言う。

## 長い道のり

ハッキング行為は、アトリビューションの公表（「パブリック・アトリビューション」と呼ばれる）が真剣に検討されるようになる数十年前から、国際政治の重要な一側面だった。だが、民間企業による画期的なサイバーセキュリティ報告書が公表され、ニューヨーク・タイムズ紙の一面に大々的に取り上げられたことで、ハッカーの正体を明らかにすることへの世界全体の考え方が変わった。

2013 年、米国のサイバーセキュリティ企業マンディアント（Mandiant）は、中国のハッカー集団「APT1」に関する報告書を公表した。史上初めて、主権国家を名指ししたパブリック・アトリビューションだった。だが、APT1 のハッキングが始まったのは 2002 年。公表までには丸 10 年もかかったのだ。

公表された APT1 に関する報告書は非常に詳細なもので、中国人民解放軍 61398 部隊として知られるサイバー・スパイ部隊による活動であることまで明らかになった。その 1 年後、米国企業の知的財産に対するハッキングおよび窃盗の罪で 61398 部隊の将校 5 人を起訴したことで、米国司法省は事実上、この報告書の内容を裏づけた。

「APT1 報告書は、サイバー攻撃者がリスクと有益性をどう計算するかを根本から変えました」。ドイツのサイバー情報調査官で、『Attribution of Advanced Persistent Threats（持続的標的型攻撃 =APT= のアトリビューション）』（2020 年刊、未邦訳）の著者であるティモ・ステフェンズは話す。

「APT1 報告書以前、サイバー作戦はほぼリスクのないツールだと見られていました。報告書は（実行犯や手法の）仮説を提示しただけでなく、明確かつ透明性のある分析手法やデータソースを示しています。これが 1 回限りのまぐれ当たりで

はなく、他の活動や攻撃にも応用できるものであることは明らかでした」（ステフェンズ調査官）。

この大きなニュースの影響は広範囲におよんだ。その後、同様のアトリビューションが続き、米国は中国が組織的かつ大規模な窃盗をしていると非難した。2015 年、中国の習近平国家主席が米国を訪問したときには、サイバーセキュリティが最重要テーマになった。

「APT1 報告書以前、アトリビューションは誰もが認識しているけど触れようとしない、いわば『部屋の中の象（見て見ぬふり）』状態でした」とステフェンズ調査官は話す。「技術的なブレークスルーのみならず、最後の段階に踏み込んで結果を公表することは、筆者と責任者が成し遂げた勇敢な功績でもあったと私は考えています」。

諜報官たちは技術面には精通しているが、最後の段階に踏み込むという部分が欠けていた。情報分析官はサイバー攻撃のアトリビューションのため、ハッカーが使用したマルウェア、攻撃を実行するために構成したインフラやコンピューター、機密情報や傍受した通信といった幅広いデータを調査する。そして「cui bono（クゥイ・ボォーノ）」、つまり誰が利益を得るのかを質し、攻撃の裏にある戦略的動機を地政学的に分析する。

データが多ければ多いほど、パターンが形成されてアトリビューションも容易になる。世界最高レベルのハッカーでさえ、間違いを犯したり、証拠を残したり、古いツールを再利用したりするからだ。ハッカーの正体を暴くための新しい方法を考え出すアナリストと、痕跡を隠そうとするハッカーの間では軍拡競争が続いている。

だが、ロシアによるサイバー攻撃に関する今回の迅速なパブリック・アトリビューションは、これまでの公表の遅れが単なるデータやエビデンスの欠如によるものではなかったことを示している。それは政治的なものだった。

「要するに、政治的意思の問題なんです」。2019 年までホワイトハウスで勤務していたワイルド元局長は言う。「アトリビューションの公表には、あらゆるレベルで断固たるリーダーシップが必要です。ノイバーガー副顧問との 交流から分かるのは、彼女は結果を出す必要がある時には

最善を尽くし、官僚的形式主義を打破していくタイプだということです。それがノイバーガー副顧問なのです」。

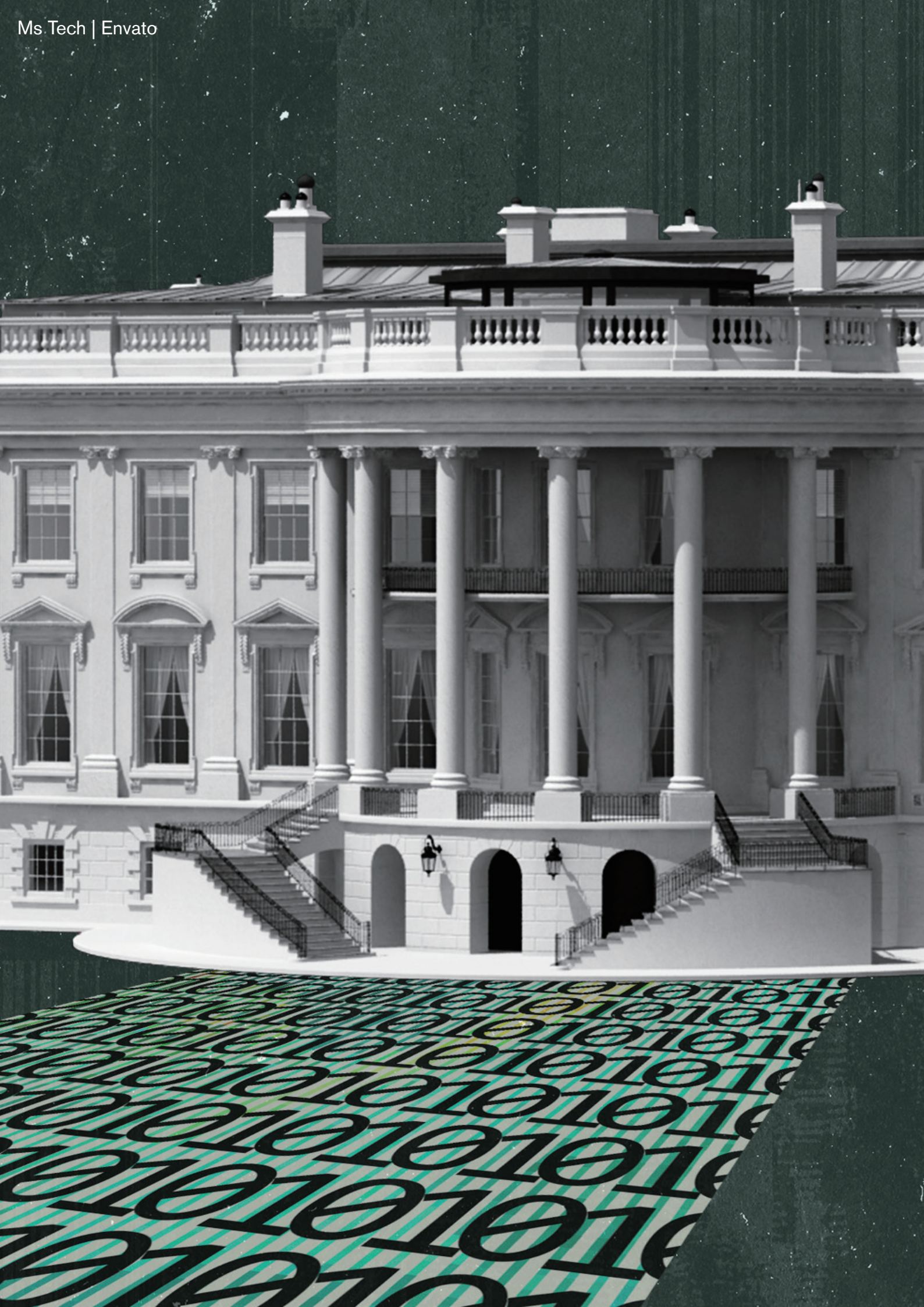
ロシアによるウクライナ侵攻で数十万人の命が危機に曝されていることで、ホワイトハウスはより迅速に行動を起こす方向に向かっているとワイルド元局長は主張する。

「バイデン政権は、サイバー侵攻であれ偽旗作戦（なりすまし軍事行動）や嘘の口実であれ、最善の防御策はそれらの作り話に先んじて効果的な先制攻撃をすること、つまり（やり口の公表という）先手を打ち、世界中の人々に予防線を張っておくことだと判断したようです」。

パブリッシング・アトリビューションは、敵方のサイバー戦略に大きな現実的な影響を与える可能性がある。攻撃者に行動を監視・把握されているという警告を与えたり、活動が暴露された際にツールを破棄して一からやり直さなければならないといったコスト面での負担を強いたりする可能性を秘めている。また、銀行口座の凍結などの制裁といった、政治的な動きにつながる可能性もある。

同じく重要なのは、政府が悪意あるサイバー活動を詳細に追跡し、起訴状や情報活動報告書をいつでも国民の目に触れるようにすることだ。それが、解決に取り組んでいる姿勢を伝えるメッセージになるとワイルド元局長は主張する。

「特にロシアや中国との間に信頼感のギャップが生まれます。彼らがどれだけ事態を分かりづらくしようとしても、米国政府はその取り組みのすべてを明らかにしていきます」。（Patrick Howell O'Neill）



# 転換期を迎えた米サイバーセキュリティ政策、規制強化の舞台裏

by Patrick Howell O'Neill

米国政府はこれまで、サイバーセキュリティ対策を民間企業の自主的な努力に頼ってきた。しかし、インフラ企業を襲ったランサムウェア被害やロシアのハッカーの脅威を目の当たりにした今、規制強化に舵を切りつつある。

2021年、米国最大の燃料パイプラインであるコロニアル・パイプライン（Colonial Pipeline）がハッキングされた。パニック状態に陥った何千人もの米国人がガソリンを買いだめし、東海岸全域が燃料不足に陥った。ハッカーの侵入を許したのは、サイバーセキュリティ上の基本的なミスが原因であった。コロニアルは、事態の収拾を図るときになるまで米国政府に何の相談もせず、一方的な判断により、500万ドルの身代金を支払い、東海岸の燃料供給の大部分を停止した。

元英国サイバーセキュリティ大臣であったキアラン・マーティンは、この様子を、大西洋の対岸から困惑した様子で見ていた。

マーティン元大臣は、「コロニアルへのハッキングに関しては、同社が商業的利己主義の狭い観点から決定を下し、後始末をすべて米国連邦政府が引き取ったものだと、厳しく評価しています」と言う。

現在、ホワイトハウスの現サイバー長官を含む米国のサイバーセキュリティ高官の一部は、サイバーセキュリティ面での政府の役割および規制を強化する時期が来ていると考えている。 コロニアルのような大失敗を繰り返さないためだ。

この方針転換は、ウクライナで戦争が起こり、ロシアからの新たなサイバー攻撃の脅威が高まるなか、ホワイトハウスが国家の安全を守る方法を見直す必要に迫られている矢先に起こった。

米政府の国家サイバー長官を務め、バイデン政権のサイバーセキュリティ最高顧問であるクリス・イングリスは、ロシアのウクライナ侵攻後の初の取材で「私たちは転換点に来ています」とMIT テクノロジーレビューに語った。「社会に必要な重要機能が問題になっている時には、自由が制限されることもあります」。

米政府の新しいサイバーセキュリティ戦略は、政府の監督強化の在り方、組織に最低限のサイバーセキュリティ基準を満たすことを義務付ける規則、民間企業との緊密なパートナーシップ、現在の市場優先アプローチからの脱却、新規則の遵守を担保するための執行方法などで構成されている。この戦略は、大気浄化法（Clean Air Act）や米国食品医薬品局（FDA）の設立など、米国で最も有名な規制事例に倣うことになるだろう。

ロシアのハッカーによる脅威が迫る中、米国連邦通信委員会（FCC）はロシアのハッカーがインターネット通信を乗っ取る可能性を想定している。これは過去にもロシア政府が採用した戦術だ。3月 11 日に発表された米国連邦通信委員会の新しい施策 は、米国の通信会社がこの脅威に対して十分な安全対策をしているかどうかを調査することを目的としている。しかし、企業に遵守を強制する力がない同委員会にとって、これは厳しい試練となる。遵守させるためには、国家安全保障上の危機が発生する可能性を説明するほかないからだ。

多くの政府関係者は、市民の安全を守るために市場の善意にほぼ全面的に頼らざるを得ない現在の状況を継続させることはできないと考えている。

オバマ政権のサイバーセキュリティ担当高官だったスザンヌ・スポルディングは、「これまで何十年間も取り組んできましたが、サイバーセキュリティに関しては自主性に頼るというやり方のために、端的に言って、あるべき姿に到達できていません」と言う。「外部性（日本版注：ある主体の意思決定や行為が第三者に影響を与えること）は、これまで長い間、公害や高速道路の安全性に関する規制や義務付けを正当化してきました」。

重要なのは、ホワイトハウスの高官の意見がそろっていることだ。イングリス長官は、「スザンヌの言うとおりです。同意します」と述べる。

この意見の支持者たちは、抜本的な変化がなければ、歴史は繰り返されると主張する。

サイバーセキュリティとプライバシーの問題に関して議会で最も発言力のある議員の１人であるロン・ワイデン上院議員は、「企業が強力なサイバーセキュリティの規則を望んでいないことは周知の事実です」と言う。「米国のサイバーセキュリティが今のような状態になっているのはそのせいです。現状を変えることがあたかも簡単なことのように言うつもりはありません。しかし、今のあり方を続けるということは、ロシアや中国、さらには北朝鮮のハッカーに、米国全土の重要システムを開放することなのです。次のハッキングがコロニアル・パイプラインを超える被害をもたらさないことを心から願います。しかし、議会が真剣に取り組まない限り、それはほぼ避けられないでしょう」。

転換は簡単ではない。政府内外の多くの専門家が、下手な規制をすればメリットよりも弊害が多くなることを懸念している。規制当局にサイバーセキュリティの専門知識がないことに不安を感じている当局者もいる。例えば、運輸保安局の最近のパイプラインに関するサイバー規制は、「ひどい」規制だと批判されている。この規制が柔軟性に欠け、不正確であり、解決するよりも多くの問題を引き起こすという理由によるものだ。批判者は、規制当局は大きな権限を持っているが、仕事を正しく遂行するための十分な時間、資源、専門性の高いスタッフを抱えておらず、その結果、このようなことになったと指摘する。

2020 年まで米国国家安全保障局（NSA：National Security Agency）の顧問弁護士を務めていたグレン・ガーストールは、現在の散発的な取り組み、つまり異なる規制当局がそれぞれの分野で別々にしている取り組みはうまくいかないと述べる。そして、異なる重要な産業に対して横断的に対応でき、専門知識とリソースを備えた、１つの中央サイバーセキュリティ当局が米国には必要だと主張している。

パイプライン規制に対する反発は、このプロセスがいかに困難であるかを物語っている。しかし、それにもかかわらず、セキュリティ上での失敗お

よび逆方向のインセンティブが散見されるような現状は、長続きしないだろうという共通認識が広まっている。

## 画期的な法律

コロニアル・パイプラインの事件は、多くのサイバー専門家がすでに知っていることを証明した。それは、ほとんどの攻撃は、古くから知られている脆弱性をハッカーたちがうまく狙ったものであり、企業が投資や解決を怠ってきた結果であるということだ。

2020 年まで国家安全保障局の顧問弁護士を務めていたグレン・ガーストールは、「良いニュースは、これらの問題を解決する方法を、私たちは実は知っていることです」と言う。「サイバーセキュリティの問題は解決できます。費用がかかり、難しいかもしれませんが、私たちはどうすればよいかを知っています。技術の問題ではないのです」。

近年のもう 1 つの大規模なサイバー攻撃も、この点を証明している。米国政府や大手企業に対するロシアのハッキング活動「ソーラーウインズ（SolarWinds）」は、被害を受けた組織が、既知のサイバーセキュリティ基準に従っていれば無力化できたはずだった。

「サイバーセキュリティの重大事件を起こしたハッカーの能力は誇張され、あたかも自然災害や神の仕業のように語られる傾向があります」とワイデン上院議員は言う。「これは便利な方便です。そう語ることで、ハッキングを受けた組織やそのリーダー、政府機関の責任が免除されるからです。しかし、事実から繰り返し明らかになっていることは、ハッカーが最初の足がかりを得られているのは、被害を受けた組織がパッチを更新せず、ファイアウォールを正しく設定していなかったためです」。

ホワイトハウスは、多くの企業がサイバーセキュリティに十分な投資を自前でしておらず、するつもりもないことは明らかだと考えている。過去 6 カ月間にバイデン政権は、銀行・パイプライン・鉄道システム・航空会社・空港を対象とした、

新しいサイバーセキュリティ規則を制定した。バイデン大統領は昨年、連邦政府のサイバーセキュリティを強化するためのサイバーセキュリティ大統領令に署名し、政府に対して納品するすべての企業に対し、セキュリティ基準を満たすことを求めることにした。民間企業を変えることは、より難しい課題であり、そして間違いなくより重要な課題でもある。最重要社会基盤や技術システムの大部分は、民間企業のものであるからだ。

新規制のほとんどは、本当に基本的なことを求めているだけであり、政府の干渉としては軽いものに相当するが、企業からは反発を受けている。そうであっても、規制が今後、ますます増えることは明らかだ。

「米国のサイバーセキュリティの残念な現状を改善するために必要なことは、大きく分けて3つあります」とワイデン上院議員は言う。「1つめは、サイバーセキュリティ最低基準の規制当局による強制、次に、被監査対象企業から選ばれていない独立監査人によるサイバーセキュリティ監査の義務化および結果の規制当局への報告、そして最後に、基本的なサイバー対策を怠った結果侵入された場合の上級役員への懲役刑を含む厳しい罰です」。

3月15日に法制化された新たなインシデント報告義務化規制は、その第一歩と見られている。この法律は、民間企業に対して、共有すべき脅威に関する情報を迅速に共有することを求めるものだ。このような情報はこれまで、たとえそれが社会的な防衛力の強化に役立つことが多いとしても、内密にされていた。

過去の規制の試みは失敗に終わってきたが、今回、新たな報告法を求める動きが活発化したのは、マンディアント（Mandian）のケビン・マンディア最高経営責任者（CEO）や、マイクロソフトのブラッド・スミス社長といった大企業からの支持を得たからだ。これは、民間企業のリーダーたちが、規制は不可避であり、重要な分野においては特に有益なものであると考えるようになったことの兆しと言える。

イングリス長官は、新しい規則の策定と施行においては、政府と民間企業があらゆる段階で緊密

に連携することが必要だと強調する。そして、民間企業の内部からも、変革が必要であるとの共通認識が生まれてきている。

サイバー脅威の情報を共有し、より良い集団防衛を形成しようとするハイテク企業の集まりであるサイバー脅威アライアンス（Cyber Threat Alliance）を率いるマイケル・ダニエルは、「私たちはこれまで長い間、純粋に自主的な試みを続けてきました」と言う。「このような試みは、必要とされるよりも遅いうえ、うまくもいきません」。

## 大西洋対岸からの視点

イングリス長官は、米国が同盟国に後れをとっていると主張する。そして、米国が学ぶべき先駆的な政府サイバーセキュリティ機関として、英国の国家サイバーセキュリティセンター（NCSC：National CyberSecurity Centre）を挙げる。NCSCの創設者であるキアラン・マーティンCEOは、米国のサイバーセキュリティに対する取り組みを、困惑と驚きをもって見ている。

「もし英国のエネルギー会社が、コロニアルが米国政府にしたようなことをしていたら、私たちは彼らを徹底的に罵倒したでしょう」と、マーティンCEOは述べる。「英国首相にその会社の会長に電話してもらい、『私たちになんの断りもなく身代金を支払い、パイプラインを止めるとは何事だ』と言ってもらうでしょう」。

英国のサイバー規制は、銀行に対し、世界的金融ショックおよびサイバーストレスの両方に対して耐性を持つことを求めている。また、英国の大手通信会社がロシアのハッカーに「完全に所有されている」ことから、英国政府は通信会社に対する規制強化に力を入れている。マーティンCEOは、新しいセキュリティ規則によって、通信会社が過去に起こしたセキュリティ上の失敗は、違法とみなされるようになったと述べる。

だが、大西洋の反対側の米国では、状況は異なっている。通信とブロードバンドを統括する米国連邦通信委員会は、規制権限をトランプ大統領時代に大幅に後退させた。サイバー戦略のほとんどが、インターネット大手の自主的な協力に頼ったもの

となっている。

すべてを網羅する一元的な新法を作るのではなく、既存の規制権限をベースとして特定の産業に1つずつ取り組むという英国のやり方は、バイデン政権下のホワイトハウスがしようとしているサイバー戦略の方法と似ている。

「すでにある（規制）権限を使い切らなければなりません」とイングリス長官は述べる。

ワイデン上院議員は、ホワイトハウスの戦略に、強く求められている変化の兆候を見ている。

「連邦規制当局は軒並み、業界のサイバーセキュリティ慣行を規制するために、今ある権限を使うことも、議会に新たな権限を求めることも恐れています。多くの産業でサイバーセキュリティが不十分なのは当然です。規制当局は、基本的には企業の自主規制に任せてきたのですから」。

## なぜサイバーセキュリティ市場は失敗するのか

数千億ドルの市場規模があり、世界的に成長しているサイバーセキュリティ市場が、失敗に終わっている根本的な理由は3つある。

「企業はサイバーセキュリティによってどのような利益がもたらされるかを理解していません」。サイバー脅威アライアンスのダニエルはこう話す。市場が、サイバーセキュリティの効果を計測できておらず、さらに重要なことに、サイバーセキュリティを企業の利益につなげられずにいるため、多くの場合、企業は必要な資金を投入する正当性を説明できずにいる。

2つ目の理由は、秘密主義だ。企業はハッキングを受けたことを報告する必要がないため、大きなハッキングに関する重要なデータは、悪評、訴訟、議員から企業を守るために秘匿されてきた。

3つ目は、規模の問題だ。コロニアルのハッキングによって政府や社会が支払った代償は、企業自身が支払う金額をはるかに超えている。公害問題と同じだ。かつてサイバーセキュリティ担当高官だったスポルディングによると、「費用が企業としての利益には表れない」ため、問題解決に他視する市場のインセンティブは弱い。

改革を支持する人々は、政府の介入権限を強くすれば、前世紀に多くの産業で実施された改革と同様に、すべてのあり方を変えられると主張する。

国家安全保障局の元顧問弁護士だったガーストールは、現在と何か異なることをしなければならないという圧力は徐々に高まっていると見ている。

「これほどまでに意識が一致している状況は、かつて見たことがありません。今回は見た目も感触も違います。本当に変化を促すのに十分かどうかはまだ分かりませんが、温度は高まっています」。

バイデン大統領の 2021 年の 1 兆ドル規模のインフラ法案では、サイバーセキュリティ対策に対して約 20 億ドルが振り分けられた。イングリス長官はこのことを、政府がサイバーセキュリティとプライバシー領域に一歩を踏み出す「一世代に一度の機会」だと指摘する。

「デジタルインフラの回復力と堅牢性に投資する素晴らしい機会を見逃さないようにしなければなりません」とイングリス長官は主張する。「私たちは考えなくてはなりません。私たちの社会が頼っているシステム的に鍵となる機能とは何なのか？ それは市場原理だけで解決できるのか？ そして、もしそれが失敗したときに、私たちはどう判断して何をするべきなのか？ それが私たちの進むべき道です。それが何年も続くプロセスである必要はありません。危機感を持って取り組めばいいのです」

## 初出一覧

**ウクライナ「IT 軍」、ボランティア頼みの危うい現実（2022.03.07）**
https://www.technologyreview.jp/s/270285/the-propaganda-war-has-eclipsed-cyberwar-in-ukraine/

**ロシアのインターネット断絶で現実味増す「スプリンターネット」（2022.03.28）**
https://www.technologyreview.jp/s/271574/russia-is-risking-the-creation-of-a-splinternet-and-it-could-be-irreversible/

**ロシアを標的とした「抗議ウェア」、オープンソース界に衝撃（2022.03.25）**
https://www.technologyreview.jp/s/271559/activists-are-targeting-russians-with-open-source-protestware/

**ロシア「報道の壁」に立ち向かう市民、ネット広告も駆使（2022.03.11）**
https://www.technologyreview.jp/s/270437/the-activists-using-ads-to-sneak-real-news-to-russians-about-ukraine/

**SNS 駆使するネット探偵、ウクライナで民間「オシント」が活躍（2022.03.17）**
https://www.technologyreview.jp/s/271255/the-online-volunteers-hunting-for-war-crimes-in-ukraine/

**露 ウクライナ侵攻で広がるデマ、片棒を担がないためには？（2022.03.01）**
https://www.technologyreview.jp/s/269876/how-to-avoid-sharing-bad-information-about-russias-invasion-of-ukraine/

**ロシア、侵攻直前に衛星通信企業へサイバー攻撃 端末数千台破壊（2022.05.13）**
https://www.technologyreview.jp/s/275828/russia-hacked-an-american-satellite-company-one-hour-before-the-invasion/

**サイバー・アトリビューション、露ウクライナ侵攻で重要さ増す（2022.03.02）**
https://www.technologyreview.jp/s/269474/the-us-is-unmasking-russian-hackers-faster-than-ever/

**転換期を迎えた米サイバーセキュリティ政策、規制強化の舞台裏（2022.03.24）**
https://www.technologyreview.jp/s/271418/inside-the-plan-to-fix-americas-never-ending-cybersecurity-failures/


MIT テクノロジーレビュー　Special Issue Vol.43

War in Ukraine
**インターネット時代の新しい戦争**

2022 年 5 月 31 日発行

翻訳・編集　MIT テクノロジーレビュー編集部
デザイン　佐藤卓（佐藤工芸）
発行　株式会社角川アスキー総合研究所
東京都千代田区五番町 3-1
カスタマーサポート　customer-service@technologyreview.jp
※ e ムックに関するご質問、お問い合わせは受け付けておりません。