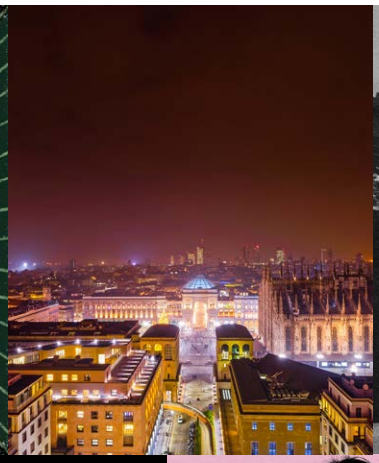
MIT Technology Review

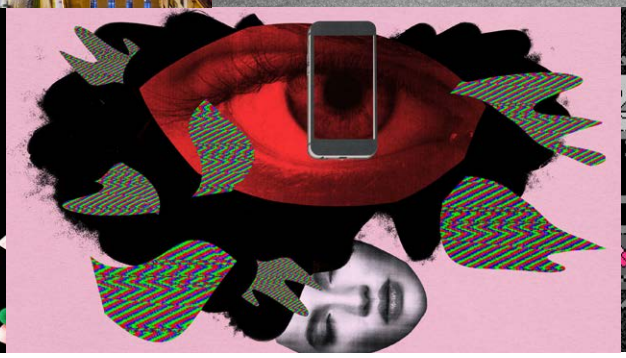
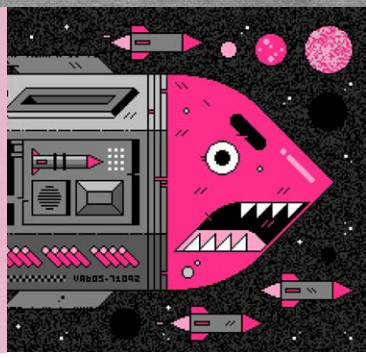
Published by KADOKAWA / ASCII

Cybersecurity

激化するサイバー戦争のリスク



サイバー攻撃の勢いが止まらない。国家が支援するハッキング集団が、送電網や産業プラント、医療機関などの重要インフラを襲い、大量の暗号通貨を盗み出しているのだ。過激化・高度化を続けるサイバー攻撃の手法と、攻撃に立ち向かう研究者の動きを紹介する。

CONTENTS

Benedikt Luft

国家が仕掛けるサイバー攻撃 2020 年は東京五輪と 米大統領選が標的に

この 10 年間にわたってサイバー攻撃の能力は拡大し続けており、
国際関係で優位に立つために国家はハッキング活動を積極的に利用するようになっている。
2020 年にはロシアをはじめとする国が、東京で開催されるオリンピックや米国大統領選挙に向けて
熾烈なサイバー攻撃を仕掛けてくるだろう。

世界アンチ・ドーピング機関（WADA）の全会一致の決定によって、ロシアが再び今後 4 年間オリンピックに出場禁止とされた時、ロシア政府は即座に怒りと反発する姿勢を見せた。ロシアが今回どのような報復に出るのか、世界は見守っている。

2016 年はロシアによる米国大統領選挙への前代未聞の妨害があった年として、歴史に残ることになるだろう。だが、それが明らかになるまで、2016 年に起こった最悪のサイバー攻撃はオリン

ピックを標的としたものだった。ブラジル・リオデジャネイロで開催された夏季オリンピック大会の直前、WADA はロシアが国家レベルでドーピングを企てたことを明らかにし、出場禁止を勧告した。これに対し、勧告を骨抜きにしようとするプロパガンダ活動の一環として、ロシア政府の最も著名なハッカーたちが、複数の国際機関を標的にして本物および改ざんされた書類をリークした。国際オリンピック委員会（IOC）はロシアの全面的な参加禁止を取り下げ、各種目がそれぞれに参加の可否を決定することを許可した。

続く 2018 年に韓国で開催された冬季オリンピック大会は、従来どおりの楽観的な気分、光り輝くライトと壮麗さで幕を開けた。だがそれに加えて、「オリンピック・デストロイヤー」として知られる、大会のネットワークと機器の妨害を目的とした標的型サイバー攻撃もあった。攻撃の発信源は偽装されており、マルウェアには北朝鮮と中国を指し示す痕跡が残っていた。だが、偽装された中身を捜査官が紐解いてみると、経験豊富なロシア人ハッカーが数人、糸を引いていることが明らかとなった。ハッカーたちは怒りのこもった一連のブログ投稿の中で、「クリーンなスポーツを守るという口実で」、「アングロ・サクソン人の秘密結社」が「スポーツの世界で権力と金」の取り合いをしていると非難した。こうしたロシア人たちは、オリンピックを世界のより大きな権力競争の一部として見ており、好んで使う武器としてハッキングに目を向けていることは明らかだった。しかし、これまでほとんど何もなされておらず、誰も責任を負っていない。

実際、一連の新刊書籍が専門的に説明しているように、サイバー攻撃の能力は拡大しており、古くからの国政術を一変させている。ロシアは、歴史を形作り、地政学的関係を自らの意志に沿ってねじ曲げるためにハッカーを使うことにおいて、米国や中国、イラン、北朝鮮などと並び競っている。

「20 年の間に、国際的なデジタル競争の場はかつてないほど攻撃的になっています」。ジョージタウン大学外交政策大学院のベン・ブキャナン教授は、近く刊行予定の著書『ハッカーと国家（The

Hacker and the State)』で書いている。「米国と同盟国はもはや、かつての方法でこの領域を支配することはできません。激烈なサイバー攻撃とデータ漏洩が、国家間に激しい闘争を巻き起こしています」。

ブキャナン教授は急速に出現しているこの駆け引きを、軍事的な対立や核競争、スパイ活動の従来の方法と学術的な視点で比較・対比し、新時代を意味づけようとしている。同書では、各国政府が「持ち札をストックしたり、または対戦相手の札を盗んで自分のために使って」、根本から「形勢を変える」ために、サイバー攻撃をどのように使うかを分析している。米国は、この目的で長らく「本拠地の強み」を利用してきた。インターネット・インフラにおける自国の中心的な地位とともに、国内の巨大テック企業と通信会社を使ってサイバー活動を可能にしているのだ。こうした活動は、米国が戦争をしたり、国連における数々の交渉を勝ち取ったりするのに役立ってきた。

一方で、ジャーナリストであるアンディ・グリーンバーグの新刊『サンドワーム（Sandworm）』は、相互に関係を持つ複数のロシア人ハッカー集団に照準を合わせている。彼らは、オリンピックを狙った攻撃だけでなく、大々的に報じられた途方もない数のハッキングに関与してきた。ウクライナでは公共設備に侵入して停電を引き起こし、米国では民主党全国委員会に侵入し、病院や港、巨大企業、政府機関を「ノットペトヤ（NotPetya）」と呼ばれるマルウェアひ1つで屈服させた。これらの大敗は、新時代を特徴づける答えのない大きな疑問を示している。つまり、何がルールなのか？ どのような結末を招くのか？ という疑問だ。

サイバー攻撃は主にネットワークやコンピューターを標的にしていると思われがちだが、インターネット上の衝突は直接的にかつ間接的に、誰にでも影響を与える可能性がある。たとえば、医療設備が障害を被ったり、私たちが暮らす地政学的現実が強制的に作り変えられたりすることが起こり得るのだ。

「今日、サンドワームやその類似集団が示している脅威の完全な姿が、未来にぼんやりと現れています」とグリーンバーグは書いている。「サイ

バー戦争の激化が野放しのままでは、国家が支援するハッキングの犠牲者は、一層悪意に満ちた破壊的な仕業の軌道に乗せられていく可能性があります。ウクライナで最初に実施されたデジタル攻撃は、ハッカーが何日も何週間も、あるいはもっと長く続く停電を誘発するディストピアが近づいていることをほのめかしています。意図的に仕組まれた電気不足が起こるのです。ハリケーン『マリア』がプエルトリコに莫大な経済的損害や人命の犠牲まで引き起こした、米国の悲劇と似たことになるかもしれません」。

新たな 10 年が始まる中、多くの米国人の頭の中にある最も差し迫った脅威は、何と言っても選挙妨害だ。2020 年の選挙における脅威は、2008 年のバラク・オバマの選挙運動のハッキングに始まり、ドナルド・トランプが外国権力のハッキングから直接的に利益を得た最初の人物となって急上昇した激化パターンを推し進める恐れがある。英国人学者のルカ・フォリスとアダム・フィッシュの近刊『ハッカー国家（Hacker States）』では、破壊の異なる側面を区別している。ハッキングは、マルウェアのインストールやアカウントの乗っ取り、データ漏洩といった特定の技術的な目的を達成したかどうかにかかわらず、人々の信用と民主主義を損なうことができるのだ。

「単なる改ざんや情報戦、影響を与える活動というだけではなく、保健医療から票集計にいたるまですべてに関わる、極めて物理的なインフラと複雑なシステムに関することでもあるのです」と、フォリスとフィッシュは書いている。

「2016 年の米国大統領選挙で、ロシア人ハッカーは 100 カ所以上の地方選挙における電子投票システムを標的にしました。改ざんが成功しなくても、あるいは、悪事を証明する情報が流出しなくても、悪意のあるコードが発見されたり、システムへの侵入が報じられたりすることで生じる疑念は、新たな陰謀じみた不安を政治に持ち込みます。そこでは、民主主義の正当性が、はっきりした答えのないままになってしまいます」。

おそらく、2020 年の米国大統領選挙に対する最も役立つ知見は、やはりオリンピックから得られるだろう。2020 年の夏季オリンピック大会は

東京で開催される。ロシア人ハッカーたちはすでに、大会をターゲットとして関係機関に対する複数のハッキングを成功させている。その活動が注目されてきたにもかかわらず、過去 4 年間ロシア人ハッカーたちがオリンピックでしてきたことに対しては、実質上何の咎めもない。したがって、同じことが繰り返される可能性は高い。

直近の 10 年間は、各国が、戦争や選挙、その他のあらゆる戦いで勝つために、ハッキングの力を利用したことで特徴づけられる。大国は自分に都合よく政治を形作るために、この極めて 21 世紀的な武器を使い続けるだろう。オリンピック競技でも選挙でも、ほんのわずかな有利さが、天と地ほどの差を生む。

その 2 つの前線における戦いが、すでに相当進行していることは間違いない。■（Patrick Howell O'Neill）

初出一覧

国家が仕掛けるサイバー攻撃 2020 年は東京五輪と米大統領選が標的に（2020/1/8）
https://www.technologyreview.jp/s/179448/hackers-will-be-the-weapon-of-choice-for-governments-in-2020/

中東の産業プラントを襲った初の「殺人」マルウェア トリトンの恐るべき手口（2019/3/29）
https://www.technologyreview.jp/s/131548/triton-is-the-worlds-most-murderous-malware-and-its-spreading/

人気暗号通貨取引所を襲った標的型攻撃、その驚くべき実態（2019/8/20）
https://www.technologyreview.jp/s/157225/an-attempted-heist-at-coinbase-was-scary-good-even-though-it-failed/

暗号通貨「両替」で資金洗浄、ブロックチェーンまたいで追跡（2019/11/6）
https://www.technologyreview.jp/s/159554/some-crypto-criminals-think-jumping-across-blockchains-covers-their-tracks-big-mistake/

米国防総省も認めた最強の「セキュリティ企業」マイクロソフトの実力（2020/2/19）
https://www.technologyreview.jp/s/180090/inside-the-microsoft-team-tracking-the-worlds-most-dangerous-hackers/

あなたを襲う「ストーカーウェア」の知られざる脅威（2019/8/16）
https://www.technologyreview.jp/s/152338/how-stalkerware-apps-are-letting-abusive-partners-spy-on-their-victims/

相次ぐ半導体の脆弱性で明るみになったパッチ「遅すぎる」問題（2019/6/6）
https://www.technologyreview.jp/s/145399/cybersecurity-flaws-in-chips-are-still-taking-too-long-to-fix/

チップの脆弱性はソフトウェアでは塞げない、グーグル研究チーム（2019/4/17）
https://www.technologyreview.jp/s/128196/chips-may-be-inherently-vulnerable-to-spectre-and-meltdown-attacks/

ハッキングされた「ハッキング・チーム」崩壊と再建のシナリオ（2019/12/25）
https://www.technologyreview.jp/s/174329/the-fall-and-rise-of-a-spyware-empire/

登場から 20 年、DDoS 攻撃を防ぐのはなぜ難しいのか？（2019/5/8）
https://www.technologyreview.jp/s/137153/the-first-ddos-attack-was-20-years-ago-this-is-what-weve-learned-since/

「宇宙戦争」の始め方――人工衛星軌道上の危ない現実（2019/11/22）
https://www.technologyreview.jp/s/159125/how-to-fight-a-war-in-space-and-get-away-with-it/

MIT テクノロジーレビュー　Special Issue Vol.25

Cybersecurity
激化するサイバー戦争のリスク

2020 年 2 月 27 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。