Wedge Special Report

日常から国家まで
今日はあなたが狙われる

いまやすべての人間と国家が、サイバー攻撃の対象となっている。
国境のないネット空間で、日々ハッカーたちが蠢き、さまざまな手で忍び寄る。
その背後には誰がいるのか。彼らの狙いは何か。その影響はどこまで拡がるのか――。
われわれが日々使うデバイスから、企業の情報・技術管理、そして国家の安全保障へ。
すべてが繋がる便利な時代に、国を揺るがす脅威もまた、すべてに繋がっている。

文・インタビュー　山田敏弘、吉岡克成、大澤 淳、ハイム・トメル、山崎文明、
川口貴久、中谷 昇、Wedge編集部（濱崎陽平、鈴木賢太郎、野川隆輝）
イラストレーション　管 弘志

CHRIS ROGERS/GETTY IMAGES

国民生活から国家までを揺さぶるサイバー空間の闇

巧みな技法を用いたサイバー攻撃が増加し、世界で被害が深刻化している。偽サイトから企業・国家への妨害まで、われわれの隙が狙われている。

文・**山田敏弘**
Toshihiro Yamada
国際ジャーナリスト

講談社、ロイター通信社、ニューズウィーク日本版などを経て、米マサチューセッツ工科大学（MIT）の客員研究員として国際情勢やサイバー安全保障の研究・取材活動に従事。著書に『世界のスパイから喰いモノにされる日本』（講談社＋α新書）、『死体格差 異状死17万人の衝撃』（新潮社）など。

者は国内外のサイバー攻撃の動向を長く見てきたが、現在ほど多くの人がサイバーセキュリティーの重要性を切に感じるようになったことはなかったのではないだろうか。ここ1年ほどを振り返っても、甚大なサイバー攻撃被害が世界各地でいくつも明らかになっている（表）。

例えば、2020年12月、米ソフトウェアの「ソーラーウィンズ」が〝史上最大級〟とも言われるハッキング被害を受けた。企業などのITシステムを遠隔で一括管理できる同社のサービス「Orion」が狙われ、契約していた1万社以上の企業だけでなく、米財務省、国防総省、国土安全保障省などの米政府機関もターゲットとなり、一部情報が盗まれた。

21年5月には、米最大の石油パイプ

インタビュー　吉岡克成 Katsunari Yoshioka

コロナ感染と相似形 生活インフラを脅かすIoT攻撃

あらゆるものがネットにつながる時代。入り口のセキュリティーが弱いとどうなるか。IoT機器への攻撃を研究する第一人者が警告する「無症状患者」の怖さとは。

聞き手／構成・編集部（濱崎陽平）

なさんは、ご家庭にあるルーターにパスワードを設定しているだろうか？　ルーターをはじめ、そのネットワークにつながったテレビやウェブカメラ、AIスピーカーなどのIoT（Internet of Things）機器類。セキュリティーの脆弱なものはハッカーに侵入されてしまう。

**　機器そのものがサイバー攻撃にあって乗っ取られるだけではなく、この機器類を踏み台に、別の機器への攻撃に勝手に加担させられている場合もある。情報通信研究機構（NICT）のサイバー攻撃観測システム「NICTER」が2019年に観測したサイバー攻撃の対象は、ウィンドウズや仮想通貨を狙った攻撃を抑え、約半数がIoT機器を狙ったものだった。**

**　IoT機器の脆弱性を研究している国内の第一人者が、横浜国立大学の吉岡准教授だ。吉岡氏は脆弱な「囮IoT」機器をわざと設置して、どういった攻撃を受けるかを研究している。IoT機器への攻撃の実態を聞いた。**

編集部（以下、――）　IoT機器への攻撃動向を調べる実験とはどのようなものか。

吉岡　ルーターやカメラといったIoT機器にパスワードをかけないなど、わざとセキュリティーを脆弱にしておき、これらにどのような攻撃が仕掛けられるかを観測している。この仕組みを「ハニーポット」と呼んでいる。

　この実験は世界の研究機関の中でも先駆けで、2015年に開始した。6年間で約17カ国の国・地域に設置し、これまで20万件を超えるマルウェア（悪意ある不正なプログラム）検体を収集した。囮として置いたIoT機器を攻撃者たちが遠隔操作したり、それを踏み台に別の機器への攻撃に使用したりしてくる。

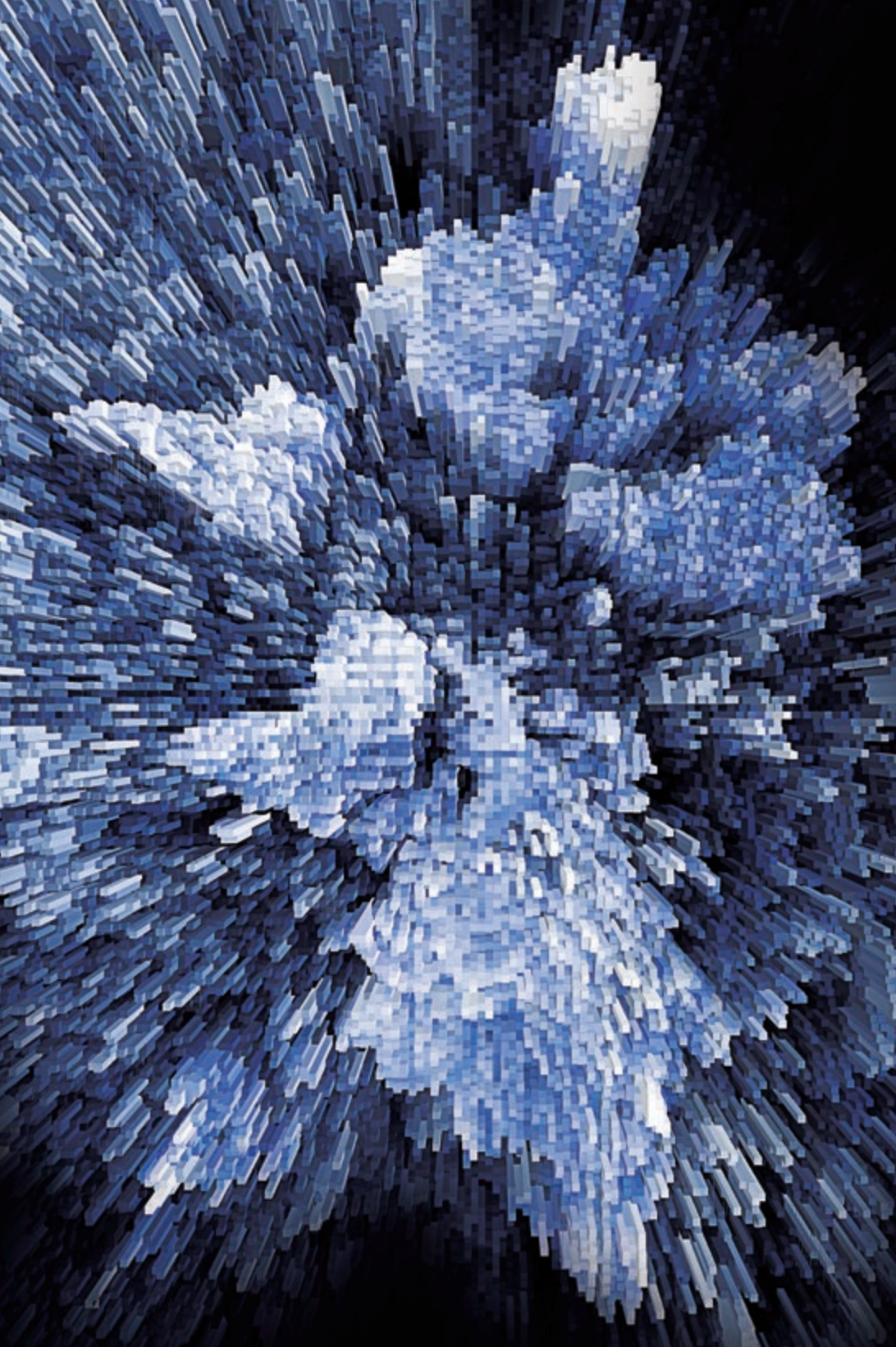
――IoT機器への攻撃の傾向は変わっているのか。

吉岡　大きくは変わっていない。IoT機器類への攻撃として有名なのは、「Mirai」と呼ばれるマルウェアを用いたものだ（編集部注・16年、米国の20代の3人組が作成したマルウェア。遠隔操作できるIoT機器類を60万台も支配下に置き、DDoS攻撃〈大量のデータを送りつけてサーバーに負担を与えて妨害する攻撃〉を行った）。

　この件で犯人は逮捕され、以降大きな被害が出ていないので、報道もされないし、話題にもなりにくい。ではIoT機器への攻撃がなくなったのかというと、決してそうではない。新型コロナウイルス同様、「変異種」がたくさん出ている。実際、海外のオンラインサービス事業者などが被害にあっている。もっと大々的に報じられれば利用者のセキュリティー感度も上がるのだが、そうではないために特に意識されない。ハッカーたちには都合のいい

吉岡克成 Katsunari Yoshioka
横浜国立大学
大学院環境情報研究院・
先端科学高等研究院准教授

2005年に横浜国立大学で工学博士号取得。情報通信研究機構研究員などを経て、11年に現職。産業技術総合研究所の客員研究員なども兼務。専門分野は情報システムセキュリティー、サイバーセキュリティー、マルウェア対策。21年より横浜国立大学情報セキュリティー統括責任者（CISO）。



Part 2

主戦場となるサイバー空間 〝専守防衛〟では日本を守れない

「宣戦布告」はなく、平時から事実上の〝開戦〟状態となるハイブリッド戦争。近隣諸国がサイバー戦力増強を進める今、日本は自国の脆弱性を直視し真正面から向き合うべきだ。

台湾有事や朝鮮半島有事が起きれば、戦闘機はもとより、ミサイルが飛び交うことも想像に難くない。しかし、実際の危機は、こうした目に見える兵器が登場する以前の平時・グレーゾーンにおける「サイバー空間」から始まる。そこに「宣戦布告」はない。これが現代の戦いを象徴する〝ハイブリッド戦争〟であり、平時から静かに忍び寄ってくるのである。

ハイブリッド戦争が注目されたのは、2014年のクリミア危機において、ロシアがウクライナ領・クリミア半島の無血占領に成功したのがきっかけであった。クリミア危機の最中には、インターネットや携帯・固定電話の遮

湾や朝鮮半島など日本の周辺地域で、安全保障環境が急速に悪化している。

文・大澤 淳
Jun Osawa
中曽根康弘世界平和研究所
主任研究員

慶應義塾大学法学部卒業、同大学院修士課程修了。専門は国際政治学（戦略評価、サイバー安全保障）。外務省政策調査員、米ブルッキングス研究所客員研究員、内閣官房国家安全保障局参事官補佐、同局シニアフェローを経て現職。

Part 3

モサド元高官からの警告「脅威インテリジェンス」を持て

**組織にとってのリスクを洗い出し、事前にリスクを排除する。
セキュリティー先進国・イスラエルが重視する積極的な防衛策とは。**

文・**ハイム・トメル**
Haim Tomer
元モサド・インテリジェンス部門トップ

29年間、モサド（イスラエル諜報特務庁）に勤務。2007～14年にモサドのインテリジェンス部門の最高責任者を務めた。

イスラエルは世界でも非常に進んだサイバー国家の一つである。その理由として、サイバーセキュリティー業界の内部から、新たな成長が生み出されるシステムが確立しているからだ。ハイテク業界も国内外からのベンチャー投資によって成長が著しく、次々と新しいビジネスが誕生する基礎となっている。

また男女ともに徴兵制がある。その過程で多くの若者がサイバーセキュリティーの実践に触れる。兵役が終われば、身につけたトップクラスの経験をもとに、民間セクターでのイノベーションを後押しする。イスラエルでは、情報機関であるモサド（諜報特務庁）が注視しているように、敵国と継続的に軍事的な紛争を続けており、サイバー領域での攻撃にも対応している。それが実務経験となって生きていく。

こうした国家的なサイバーセキュリティー戦略において、敵と対峙するために常に次のレベルのインテリジェンス活動を求めてきた。それにより高いスキルを持つサイバー攻撃者を生み出している。

イスラエルでは2012年、首相府に国家サイバーセキュリティー局（INCB）が設立された。18年にはそれが国家サイバー総局（INCD）となり、イスラエルのサイバー防衛とサイバー領域の強化に責任を持つ、国家的に非常に重要な政策がとられている。安全で開かれたサイバー空間を維持するため、モサドやイスラエル国防軍が安全を担っている。

サイバーセキュリティーにおいて、われわれは今、大変な時代を生きている。民間企業も公的組織も、大企業も零細企業も関係なく、かつてないサイバー攻撃の脅威に晒されているからだ。サイバー犯罪は体系化され、不正アクセスによって手に入れたデータを収益化するというシンプルな目的を果たすために、攻撃者は次なるターゲットを探し続けている。

普段私たちは一般的なブラウザーを使ってインターネットにアクセスしているが、そこはサイバー空間の表層的

GABI LUK AS/GETTY IMAGES

Part 4

狙われる海底ケーブル
中国サイバー部隊はこう攻撃する

中国のサイバー戦を担う戦略支援部隊。台湾有事では海底ケーブルの切断が懸念されている。忍び寄るリスク、起こりうる事態を想定し、日本も台湾有事に備えるべきだ。

文・**山崎文明**
Fumiaki Yamasaki
情報安全保障研究所首席研究員

明治大学サイバー研究所客員研究員。元会津大学特任教授。1978年、神戸大学海事科学部卒業。損害保険会社を経て大手外資系会計監査法人でシステム監査に長年従事。システム監査、情報セキュリティー、個人情報保護に関する専門家として、政府関連委員会委員を歴任。

台湾有事が勃発する可能性が高まっている。早ければ、2024年1月の台湾総統選で、蔡英文総統か台湾独立派の人物が優位に立つということがわかった時点で、中国による台湾封鎖、台湾侵攻が行われることも考えられる。中国による台湾封鎖が始まれば、一気に台湾は中国の手に落ちる可能性がある。

中国共産党が台湾侵攻を図るとしても、あくまでも短期的な地域紛争にとどめたいというのが本音であろう。米国や日本の軍事介入を避けて、本格的な戦争にまで発展しない形で台湾を取りに行きたいはずだ。ロシアがクリミア併合をほぼ無血で成し遂げたように、物理的な攻撃は最低限にとどめ、サイバー攻撃や世論操作など、いわゆる情報戦を組み合わせたハイブリッド戦争を理想としている。

中国人民解放軍がハイブリッド戦争の概念を最初に打ち出したのは、中国人民解放軍大佐の喬良と王湘穂が1999年に発表した論文『超限戦』である。そして、政治、経済、文化、思想、心理など社会を構成するあらゆる要素を兵器とするという考えが示されているこの論文を具現化した組織が、2015年12月に設立された中国人民解放軍戦略支援部隊である。

戦略支援部隊は中央軍事委員会に直属し、人民解放軍全体を支援している。中国の19年の国防白書には、「鍵となる領域において一足飛びの発展を推進し、新型の作戦戦力の加速された発展と一体的な発展を推進し、強大かつ近代化された戦略支援部隊の構築に努める」との目標を掲げている。

戦略支援部隊は、軍事宇宙作戦の責任を担う宇宙システム部と「情報作戦」の責任を担うネットワークシステム部で構成されている。ネットワークシステム部はサイバー戦、技術偵察、電子および心理戦の責任を担っており、これらの任務を同一の組織傘下におくことで、「網電一体戦」と呼ぶサイバー要素と電磁波を利用して行われる電子

日本企業の技術は、悪意のある第三者から見れば宝の山。技術流出を防ぐために必要なこととは？
ESCHCOLLECTION/GETTYIMAGES

WEDGE REPORT

経済安保に直結する輸出管理 日本企業の技術流出を防げ

日本企業、とりわけ中小企業には多くのニッチで高い技術がある。
企業の輸出管理の実態と浮かび上がる課題は何か。最前線の現場を歩いた。

文・**編集部**（友森敏雄）

「通常、自前でサプライチェーンを把握しようと思っても2次、3次までが限度であり、多額のコストもかかる。だが、この技術を使えば、10次にまでさかのぼることができる」。こう話すのは、データ解析企業フロンテオ（東京都港区）の守本正宏社長だ。インターネット上にあるIRなど企業の公開情報から個社のサプライチェーンをAIで分析するというもので、今年10月5日のサービス開始以来、大企業を中心に問い合わせが殺到しているという。

このサプライチェーン解析システム「セイズアナリシス」を使えば、米国の制裁リスト（エンティティー・リスト）に掲載された企業が自社のサプライチェーンに入っているか否かがたちどころに分かる。兵器関連企業でエンティティー・リストに入っている「中国南方工業集団」と、日本企業の取引を調べると、直接取引である1次では0件だが、2次で10件、3次で135件、4次で575件と、間接的につながっている実態が浮かび上がる。

AIが分析したサプライチェーン情報はあくまで予測であるため、その精

WEDGE REPORT

「親の義務」から「社会の責任」へ 子育て先進国・フランスに学べ

日本と同様に少子化問題に直面しながらも、その後のV字回復に成功したフランス。
子育て世代に対する厚遇を支えるのは「子どもは社会で育てるもの」という、国民の共通理解だ。

文・**高崎順子** Junko Takasaki
在仏ライター

CATHERINE DELAHAYE/GETTY IMAGES

「次世代を担う〝芽〟をいかに育むか」は、新型コロナ同様、世界共通の課題である

コロナ禍で少子化が加速する日本。2020年の合計特殊出生率は1・34、出生数は約84万人と5年連続の低下となった。自民党の総裁選では候補者4人が「子育て関連の予算を倍増する」と訴えたが、衆院選を終えた今、新政権はいかなる発想と姿勢で、この国難に臨むべきか。それを考えるために好材料となるのが、ここ20年で少子化改善に結果を出してきたフランスだ。

フランスも日本同様、20世紀後半から合計特殊出生率の連続降下を経験し、1993年には1・66の最低値を記録した。しかしそこから後述するさまざまな国策を講じたことで、2010年には2・02まで数値を回復させている。その後は不況、連続テロ、気候変動など複合的な社会不安と新型コロナウイルス流行の影響を受けて微減が続き、20年の合計特殊出生率は1・84となっているが、それでも欧州連合(EU)トップ国の地位を維持している。

フランスで「子どもが多く生まれている」という実態は、20年の出産年齢女性数と出生数で日仏を比較すると、より強く伝わるだろう。20〜44歳女性