サイバー空間

緩やかな規制と政府の役割

姿の見えない敵に苛まれ、サイバー空間のセキュリティをめぐる闘いは終わりがない。
しかし、自発的に下から積み上げられてきたこれまでの「文化」を無視すれば、空間そのものの意義が失われる。政府は何ができるのか。

外務省大臣官房情報通信課長
三澤 康
みさわ やすし
一九八五年京都大学卒業、外務省入省。アジア大洋州局大洋州課長、経済局政策課長、内閣官房副長官補付などを経て、二〇一一年八月より現職。

私が外務省に入省したのが一九八五年。東西冷戦の終盤で、バブル経済の入り口。情報化時代が始まり、アルビン・トフラーの『第三の波』が広く読まれていた。あれから四半世紀経過した二〇一一年八月、私は入省後はじめて情報通信分野をフォローする仕事についた。そして最新事情を眺めると、四半世紀の間の革命的な変化を感じる。

最大の変化は、グローバルな通信ネットワークの出現と情報量の拡大である。通信インフラの発達で大量の情報が瞬時に移動可能となり、あらゆる情報がネットワークに集中している。二つ目の驚くべき変化は、ネットワーク上の情報の力である。単なる知識としての情報ではなく、金融取引を実現させる情報や、さまざまな機器を作動させる情報、プログラム化され自ら作動する情報などが、社会や経済を直接動かす力を持ち、生き物のように動き回る。三つ目は、ネットワーク上のハードやソフトの多様化と、個人の台頭である。昔は大型コンピューターや据え付け型パソコンが主であったが、最近はスマートフォンやタブレット型端末など機能性が高く携帯性に優れた端末が出現し、個人が情報を扱う主役に躍り出た。個人が、ネットワーク上の情報を駆使し、多様な機器を動かし、人やお金を動かし、

クラウドを利用して高度な処理能力を手に入れる。

「サイバー空間」は、新しく、自由で、革新的である。この空間は、未来の技術革新や経済発展につながる。しかし「サイバー空間」はしがらみがなく、自由であるがゆえに、破壊的でもある。

何が脅威なのか

「サイバー攻撃」という言葉が頻繁に使われるが、犯罪行為を含め、さまざまなタイプの「攻撃」がある。

「攻撃」の主な目的としては、①相手の信用を落とすこと、②金銭取得、③相手に物理的被害を与えることの三つがある。いずれも、攻撃を受けた個人や組織に多大な被害を与える。官民ともに、それぞれの立場で自らを守る努力をしており、また、このような攻撃から市民を守ることは政府の重要な使命である。悪意を持ってウイルスを作成する行為などは犯罪として罰せられることとなり、警察も捜査に力を入れている。しかし、サイバー空間では、技術革新が日進月歩で、現実世界とは異なり組織や政府に対する個人の力が非常に強く、攻撃側が有利な状況は否めない。その中で、組織のネットワークを預かる身としては、「サイバー攻撃」により機密情報や個人情報の漏洩や、社会的信用の失墜を阻止することが大きな課題である。

外務省の情報通信ネットワークも数多くの標的型メールによる攻撃を受けてきた。受信時に察知した場合もあれば、本物の業務メールとの見分けができずに議事録らしい添付ファイルを開封してしまったケースもある。特に最新のウイルス対策ソフトでも検知不能な未知のウイルスの侵入を水際で阻止することは容易ではない。

感染を早期に検知するため、コンピューター内部の動きや外部との通信を常時監視し、情報の流出などの被害の予防に努めるしかない。外務省の場合は、外部のウェブサイトへの接続やメール送受信ができるネットワークと、外部との接続を遮断したネットワークを有しており、前者では安全保障やインテリジェンス関係などの秘密情報は扱わない。また、外部と接続をするネットワークがウイルスに感染しても重要な情報が漏洩しないための努力も強化している。

一方、最近では情報漏洩が確認されていなくても、ウイルス感染したことだけで国内でセンセーショナルに報道される傾向がある。その結果、外国政府や海外メディアも注目する。攻撃側からすればメディアに取り上げられ、攻

撃対象の信用が落ちれば、それだけで大きな目的を達成したことになる。守る側として、報道内容に不正確な点があれば、事実関係の修正や、実施している対策を説明している。

しかし、対外的に詳細に説明すれば、攻撃者に自らの手の内を知らせることにもなるのが悩ましい。マスメディアにおいても、攻撃者に荷担する構図にならないよう、正確な情報に基づく冷静な報道や、状況改善のための課題や具体策につながる報道に力を入れてほしい。

これらの点については政府も民間企業も同じ悩みを有しており、悩みを共有する者同士、緊密に連携し最良の対策を模索する必要がある。民間においては、個別の企業・団体のセキュリティ・インシデント対応を支援するＪＰＣＥＲＴ／ＣＣや、インシデント対応チーム間での連携・協力を進めるＣＳＩＲＴなどの組織が活発に活動している。政府内においても内閣官房の情報セキュリティ・センター（ＮＩＳＣ）が中心に各省との連携を強化し、警察庁、経済産業省も民間との連携強化に努めている。外務省の情報通信システムを管理している立場からも、引き続き内閣官房が中心になり、民間とも連携しつつ省庁横断的な対策を具体化していくことを期待している。

「サイバー攻撃」の代表的な態様としては、①ＤＤｏｓ攻撃などを通じたウェブサイトの停止や改ざん、②ウイルス感染やハッカー攻撃を通じた特定情報の窃取、③ウイルス感染などを利用した特定のシステムや施設の停止や破壊などがある。これらの攻撃は相互に補完しあうもので、特に「情報の窃取」はさまざまな攻撃の準備活動になっている。

その中で、外交に携わる立場から特に深刻なのは、「特定のシステムや設備の停止や破壊」である。昨年「Ｓｔｕｘｎｅｔ（スタックスネット）」といわれる新しいウイルスが世界を驚かせた。専門家は、「Ｓｔｕｘｎｅｔ」には、イランの核開発施設にあるドイツ企業の制御装置に対してのみ作用する特殊なプログラムが組み込まれていて、実際に核兵器実用化を大幅に遅延させる効果があったという。イランの核開発施設に関わるネットワークは外部との接続はなく、一部の関係者のみがアクセスできるものと考えられる。しかし、関係者の使用するＵＳＢメモリーがウイルスに感染し、ＵＳＢメモリーを通じて核施設に繋がる内部ネットワークに感染したと考えられている。外務省も含めどの組織でも、外部からの入手情報を内部ネットワークにインプットせざるを得ない状況は発生する。その時に

「Stuxnet」のようなウイルスに感染したUSBメモリーを利用すると、内部ネットワークと繋がっているシステムを機能不全に陥らせる危険があることが明らかになった。その他にも、例えば米軍の内部ネットワークへの最も深刻な攻撃を二〇〇八年に受けていたことを、米国防省が明らかにしたが（『フォーリン・アフェアーズ』二〇一〇年九／一〇月号：ウィリアム・リン国防副長官）、そのケースでもUSBメモリーが感染媒体であったと報告されている。さらに最近では、「Duqu（デュークー）」と呼ばれる「Stuxnet」に似た新種のウイルスも発見されている。世界中のネットワーク管理者は、このように今まで安全と考えてきた内部ネットワークまで脅威が及んでいることに震撼している。

このような「サイバー攻撃」の主体は、①個人やゆるやかな個人の集合体（ネットを通じて繋がっているグループなど）、②明確に組織化された民間グループ（犯罪組織やテロ組織など）、③国家や国家に類似する組織などがあり得る。先ほど説明した「特定のシステムや設備の停止や破壊」は、東西冷戦時代の伝統的な発想からすれば「国家や国家に類似する組織による攻撃」と考えるのが妥当であった。しかし、情報の送受信の主体として、個人の役割が大きくなっているなか、「個人やゆるやかな個人の集合体」や「明確に組織化された民間グループ」が攻撃者となる可能性も高くなっている。「Stuxnet」によるイラン核施設への攻撃も、イスラエルや米国の関与に言及する説もあるが、「実は、シーメンスのライバル企業による攻撃の可能性もあるのではないか」と指摘する人もいる。また、緩やかな個人の集合体と考えられるハッカー集団も、目的を共にして活動するなかで、より強固な組織として、「特定のシステムや施設の停止や破壊」を目指す可能性もある。9・11以降、テロリストのような集団も武力紛争の主体となり得るとの議論がなされてきており、「サイバー攻撃」による脅威は、さまざまな可能性が出てきている。

なぜ「報復」が難しいのか

もし国の経済と生活の根幹を支える電力、通信、水道などの基幹インフラが「サイバー攻撃」によって破壊されたら政府はどう対処すべきか。国の安全保障を揺るがしかねない問題であり、新たな安全保障領域として国際的な議論が始まっている。

米国政府は「サイバー攻撃」による物理的な被害に対して、伝統的な安全保障の考え方に基づき「報復」を行うとしている。しかし、「サイバー攻撃」はとらえどころがない。

例えば、「サイバー攻撃」が日本の基幹インフラに壊滅的な打撃を与え、その攻撃主体が外国政府であることが明らかな場合、これを「武力攻撃」と位置づけるということもあり得るのか。その場合、このような攻撃に対する反撃はどこまで認められるのか（物理的な軍事力も行使できるのか）。また、明らかに基幹インフラを破壊する意図を持ったウイルスを含んだ標的型メールが、関連施設内のネットワークに入る直前で検知され隔離された場合はどのように考えるのか。標的となった施設に感染したが、たまたま仕組まれたウイルスが不完全で被害がなかった場合はどうであろう。また、これらの攻撃に対して、どのような防衛措置がとられるべきか。領海や領空と同じように、領土とみなすべき「サイバー空間」を定義して、その空間の防衛を国として行うべきであろうか。さらに言えば、日米安全保障条約の適用についても検討の必要があるであろうし、日本としての抑止力をどのように高めるべきか、ということも考えなければならない。

「サイバー攻撃」の本当の攻撃主体を確認することは容易ではないことも問題である。結局、大きな被害が出たにもかかわらず、その攻撃主体が明らかでない状況もあり得る。また、攻撃主体が個人の集合体である場合や、攻撃元のＩＰアドレスが外国にある場合、複数の国にまたがる場合に、安全保障上、どうとらえ、どう対応すべきか。

「サイバー攻撃」の論点は、これまでの解釈に基づく安全保障論では整理が難しい問題ばかりである。しかし、日本の防衛の観点からは、「サイバー攻撃への対処」は重要であり、すでに防衛省も体制を強化している。それと同時に、今そこにある脅威にどう現実的に対処するかという観点から、政府内のみならず、広く国内で安全保障面の議論や検討をすることが必要となっている。

伝統的ルールと市民的ルールの融合

「サイバー攻撃」に対する安全保障面での対応も重要であるが、ＩＴ大国である日本は、サイバー空間での主要な利益の享受者であり、この空間の永続的な管理の在り方について、新たな発想で世界をリードしていくことも必要である。

国際会議の場においては、サイバー空間の利点である自由を制限しても安全のために厳しいルールを作り上げるべきとする傾向の強い中国やロシアのような考え方と、ゆるやかなルールが必要と考える欧米諸国との間で意見の隔たりは大きい。個人的には、新時代の象徴でもあるサイバー

空間において、伝統的な国家の概念を持ち出し、国家による管理を強調するのには違和感がある。インターネットのＩＰアドレスやドメイン名は米国商務省の管轄下にあるとはいえ民間の非営利団体であるＩＣＡＮＮにより調整され、ＴＣＰとかＰＯＰ3などの技術標準はＩＥＴＦというネット上のボランティア団体のような組織がネットならではの緩やかな合意手続きを採用している。ウェブサイトの標準化もＷ３Ｃという非営利団体の勧告により取り決められている。サイバー空間のルールの多くはボトムアップ方式で築かれ、発展してきた。いきなり政府が強い音頭を取って無理にルールを作っても必ずしっぺ返しを食うであろう。

しかし、このようなサイバー空間の独特の自由を守るためにも、今の状況の改善、すなわち交通ルールの整備と最低限の違反の取り締まりは必要と考える。そのためには、民間の議論と並行して、各国政府の関与も不可欠である。日本は、高いＩＴ技術を有する民間企業や人材も抱えており、官民が緩やかに連携して、新しいルールにつながる技術の開発や、ルール作りに貢献していくべきである。

例えば、公道における車の利用にあたって車検や車の登録、ナンバープレートの表示が義務づけられるように、インターネットにおいても表現の自由や情報保護をしっかりと確保しつつも、利用端末と利用者をもう少し厳密に管理できないのか。誰がどの機器で情報を送信したのかがネットワーク上でチェック可能となる技術とルール（送信者が誰かの証明書がない情報の送信は遮断される等）を作れないか。その際に、量子暗号などを活用して、暗号化されている情報の中身を解読するような動きは、送受信者自らチェックできるようにできないか。日本の民間団体や企業は、このような取り組みにつながるさまざまな研究をしている。本当に役に立つものであれば、官民連携して実用化に取り組むとともに、日本単独ではなく、欧米諸国やＡＰＥＣ諸国とも協力していくことが必要であろう。

「サイバー空間」の主役はすでに個人に移っている。ルール作りも、民間企業やベンチャー企業、あるいは個人がアイデアを提案し、ローカルレベルで試みを重ね、それに国や地方自治体や他の企業がついていくような流れが理想的であろう。将来の日本社会のあり方を考える上で、このような下からのイニシアチブと、政府レベルの取り組みの連携が不可欠な分野はたくさんあるが、この分野は特に日本経済そして日本社会にとって非常に意義の大きい新たな挑戦である。■