サイバーセキュリティの地政学

慶應義塾大学　大学院政策・メディア研究科 教授　土屋（つちや）　大洋（もとひろ）

1. 大規模なサイバー攻撃被害

2017年5月15日、16日、新聞各紙にはサイバー攻撃に関する記事が並んだ。「サイバー被害150カ国に　身代金ウイルス、20万件」（朝日新聞、15日）、「交通や医療に注意喚起　世界的サイバー攻撃　政府、警戒強める」（読売新聞、15日）、「IoTの盲点突く、世界同時サイバー攻撃――接続だけで感染拡大」（日本経済新聞、16日）、「サイバー攻撃国内600カ所・2000端末感染か」（産経新聞、16日）、「サイバー攻撃：ランサムウエア、世界拡散　北朝鮮との関連調査　米露情報会社」（毎日新聞、16日）といったものである。そして、同様の見出しが翌6月にも各紙で躍ることになった。

5月の事件では、150か国、20万件とも30万件とも言われる被害規模から、多くの注目を集めることになった。これほどの規模でなければ、サイバー攻撃事件は、近年では年に何度か起きるようになっている。小さなものを含めれば、毎日のように被害が出ていると言って良いだろう。

しかし、実害はまちまちである。2017年5月と6月の事件では、ランサムウエアと言って、それに感染するとコンピュータの中身が暗号化され、鍵を手に入れないと元に戻せなくなる悪性プログラムが使われた。データを元に戻す鍵を手に入れるためにはランサム（身代金）を犯人に払わなくてはならない。

コンピュータの中のデータが取り出せなくなったり、使えなくなったりすることで、業務に支障が出たところもあるだろう。今回特に深刻だったのは、英国の医療サービスで被害が発生し、病院の業務に支障が出たことである。しかし、それでも、ランサムウエア攻撃によって直接の死者は出ていないだろう。おそらく負傷者も出ていない。仕事ができなくなったり、大事なデータが失われたりして、途方に暮れた人はいただろう。金銭的な被害もあるかもしれない。それでも、おそらくは誰も怪我をしたり死んだりはしていない。何かが爆発したということもなかっただろう。

2. 身代金強奪は失敗か

一連の事件で、身代金を払ったのは300組程度だと見られている。30万件の被害があったとして、300組だとすれば、0.1％である。払った金額の総計は1500万円程度とされている。ところが、身代金を払うことでデータを元に戻すための鍵を手に入れることができた人もおそらくいない。犯人たちはビットコインという仮想通貨で支払われた身代金を8月上旬になってようやく引き出したことが確認された。それを各国政府機関が追跡している。

つまり、金銭目的のサイバー攻撃としては大きな成功とは言えない。それは何を意味するのか。第一に、攻撃者が想定していたよりも被害が大きくなりすぎ、身代金と鍵の管理がうまくできなかった可能性がある。本来、ランサムウエアは身代金を払いそうなターゲットに絞り、ランサムウエアを感染させ、ひそかに身代金を受け取ることに意味がある。狙われたターゲットとしては、そうした被害に遭ったこと、そして身代金を払ったことを隠しておきたいはずだ。隠しておけるうちに身代金を払い、そんな事件はなかったことにしたい。だから急いで身代金を払うことになる。しかし、今回は、想定以上に感染が広がり、その管理ができなくなってしまったのかもしれない。

第二の可能性は、そもそも金銭目的ではなく、身代金を受け取ってもデータ回復のための鍵も提供する気はなく、ターゲット（あるいは広く社会内）の業務を妨害することが狙いだというものである。身代金が300ドル（3万3000円）程度だというのも気になる。大もうけという金額ではない。単純に3万円を30万組が払えば、90億円になる。しかし、実際には300組超で、1500万円にしかならなかった。その規模と手間に比して十分とは言えないのではないだろうか。狙いは金銭ではなかったのかもしれない。

5月の攻撃については、北朝鮮が国家として関与したという指摘もある。6月の攻撃については、ウクライナで被害が大きいことからロシアの関与も疑われている。今のところは北朝鮮政府やロシア政府の関与を決定付けるような証拠は出てきていないが、タイミングと意図の2つの点から、納得のいく説明はまだ得られていない。

3. ほとんどのサイバー攻撃は武力攻撃ではない

本来、国際法上の定義では、「サイバー攻撃」という際には、物理的な被害や人命への危害が伴わなくてはならな

いとされている。そうでなければ、ほとんどの事案は「サイバー犯罪」ないし「サイバー作戦」、「サイバーエスピオナージ（スパイ活動）」と呼ばれるものに過ぎない。「サイバー戦争」という言葉もよく使われるが、戦争が戦争であるためにはいくつかの条件をクリアしなければならない。例えば、国家間で宣戦布告が行われてから戦われることになるが、そういう意味でのサイバー戦争はまだ一度も起きていない。

当事者が誰なのかもわからないまま、ひそかに行われるサイバー作戦だけで従来型の戦争になる可能性はほとんどないと言って良いだろう。可能性があるとすれば、本格的な武力行使の前段階として奇襲的に使われるということになる。しかし、サイバー的な手法だけの戦争は考えにくい。

無論、サイバー作戦が絶対に物理的な破壊や人命への危害を引き起こせないわけではない。むしろ、それが可能であることはいくつかの事例で示されている。2007年3月、米国政府の国土安全保障省は「オーロラ発電機テスト」と呼ばれる秘密の実験を実施した。巨大な発電機を実験場に設置し、それを操作するためのコンピュータ・プログラムに21行書き足し、正常とは違う方法でベントを開け閉めしてみるとどうなるかを試してみた。すると、発電機は何度か音を立てて大きく振動した後、わずか数分で黒い煙を吐き出し、後の検証で全ての部品が壊れていたことが分かった。

2010年に発覚したイランの核施設に対するサイバー攻撃は、スタックスネット攻撃あるいはオリンピック・ゲームズ作戦と呼ばれるが、施設内で使われていたウラン濃縮のための遠心分離機の制御システムが不正に操作され、遠心分離機がおかしな動作をしたり壊れてしまったりした。スタックスネット攻撃を行ったのは米国とイスラエルだと報道されているが（両国政府は認めていない）、報復としてイランは米国の金融機関をサイバー攻撃したり、米国ニューヨーク州にある小さなダムの制御システムにサイバー攻撃を仕掛けたりした。

2015年12月にはウクライナ西部（西部ではロシア系住民が少ない）で大規模な停電が起き、発電網の制御システムにマルウェアが送り込まれていたことが分かった。実行者は確定していないものの、ロシア政府の関与が疑われている。

4. サイバー攻撃のアトリビューション

従来、「アトリビューション」と呼ばれるサイバー攻撃者特定は難しいと言われてきたが、全てのサイバー作戦で実行者が分からないわけではない。2012年10月、米ニューヨーク・タイムズ紙が中国の温家宝首相（当時）の蓄財疑惑に関して記事を書いたところ、同紙や米国政府・メディアに対するサイバー攻撃が行われた。それに対して同紙は2013年2月、上海のビルがサイバー攻撃の発信源となっており、そこには中国の人民解放軍の61398部隊が入っていると名指しした。さらに2014年5月には、米国司法省のエリック・ホルダー長官が記者会見し、61398部隊のメンバー5人を特定し、被疑者不在のまま起訴すると発表した。手配書には5人の実名、オンラインのハンドルネーム、写真が掲載されている。

2014年12月には米国の映画配給会社ソニー・ピクチャーズエンタテインメントがサイバー攻撃を受け、社内の各種データが漏洩した。原因は同社が配給しようとしていた北朝鮮を揶揄する映画『ジ・インタビュー』にあるとされた。米国連邦捜査局（FBI）はしばらくしてサイバー攻撃は北朝鮮によるものだとした。

さらに2014年には米国のヤフー！から5億人もの利用者情報が漏れたことが分かり、2017年3月になって米国司法省はロシア当局者を起訴した。

そして、2016年の米国大統領選挙では、米国民主党全国委員会（DNC）の電子メールデータが何者かによって盗まれ、ウィキリークスなどのサイトで暴露されるとともに、偽ニュースが拡散されるという事件も起きた。大統領選挙後の2016年12月、米国政府は35人のロシア政府関係者を米国から追放するなど、政治的な制裁を行い、米国政府はロシアからの介入があったと結論付けた。2017年7月のG20サミットでトランプ大統領とロシアのウラジミール・プーチン大統領が初の首脳会談を行ったが、プーチン大統領は関与を認めず、ロシアからのサイバー攻撃について両者の見解は食い違ったままだった。

しかし、これらの事例を見ると、完全ではないにしても、サイバー攻撃の首謀者はある程度分かるようになっていることが分かる。無論、サイバー攻撃と言われているもののほとんどは、サイバー犯罪でしかない。それらすべてのアトリビューションを解決することは現実的に無理である。しかし、国家を揺るがすような大きな事件では、各国政府、特に米国政府は総力挙げてアトリビューション問題に取り組んでいる。

5. サイバー攻撃は地政学的リスクを反映する

アトリビューション問題が徐々に解決する中で言えることは、深刻なサイバー攻撃、サイバー作戦は、地政学的なリスクを反映しているということである。

しばしば、サイバー攻撃は地球の裏側から瞬時に可能であると言われる。実際には、サイバー攻撃には入念な準備が必要である。ターゲットが外国政府である場合には、自分のアトリビューションを徹底的に隠す措置を執らなくてはならない。そして、ターゲットがどんなハードウエアとソフトウエアを使っているかを特定し、それに対応する脆弱性を見つけ、それを悪用するマルウェアや不正侵入方法を開発しておかなければならない。それができるのは資金的に余裕のある組織であり、数名の悪玉ハッカーだけでは難しい。

例えば、ゼロデイと呼ばれるメーカーがまだ把握していない脆弱性は、闇市場で1億円程度の値がつくこともある。資金と人員を確保した組織でなければできない。単なる金儲けのためにそこまで投資するのは、個人には難しいだろう。そういう点が、アトリビューションにもヒントを残すことになる。

2016年のリオデジャネイロでのオリンピック・パラリンピックでは、それほど大きなサイバー攻撃被害はなかった。そのため、2020年の東京オリンピック・パラリンピックもそれほど心配する必要はないという声もある。

しかし、ブラジルと日本のそれぞれの地政学的リスクを見る必要があるだろう。ブラジルはオリンピック開催前から大統領の弾劾問題が起きるなど、内政に多くの問題を抱えていたが、対外的な緊張関係はそれほどなかった。それに対し、日本は周辺国との間に少なからぬ緊張関係を持っている。外国政府によるサイバー作戦だけではなく、民間の組織による反日サイバー作戦も、想定されるだろう。

2012年のロンドン・オリンピックでは2億件のサイバー攻撃があったと言われているが、2020年の東京ではその数倍になってもおかしくない。特に、IoT（Internet of Things）と言われるように、日本では様々な機器がつながるようになっており、それは逆に様々なところに脆弱性が存在するということにもなりかねない。

2020年のオリンピックでサイバー攻撃が終わるわけではない。その後の東京、そして日本を守るための措置を講じるべきだろう。2018年に韓国の平昌で開かれる冬季オリンピックが注目に値する。そこでの経験は東京にも活用できる。同盟国の米国、ロンドンの経験を持つ英国だけでなく、韓国との協力も進めていくべきだろう。