**サイバー兵器競争の最前線**

テクノロジーに関する専門用語は、多くの場合、悪いニュースによって広く認知されるようになります。例えば20年前、「インターネットを破壊する」と言われていた迷惑メールの疫病神「スパム」や、現代の働き盛り世代が生まれた頃には存在しなかったサイバーセキュリティの分野自体もその一例です。

今年、そんな不吉な言葉になりそうな専門用語は「ランサムウェア」です。ランサムウェアは「スパム」や「ウイルス」同様、専門家たちの間では以前から注目されてきました。しかし、ランサムウェアは標的のシステムにすぐに組み込まれてしまうため、目立たない存在でした。被害を受けた企業も、ブランドイメージが損なわれないように、事を荒立てず、支払いを行って対処しようとします。結局のところ、パスワードをリセットしたり、盗まれたお金を顧客に返金したり（保険でカバーされることもある）する方が、企業が安全でないことを顧客に悟られるよりも安上がりなのです。また、サイバーセキュリティの専門家を採用し、セキュリティ強化に必要な改修や保守費用を継続的に払うより、身代金を渡した方が安価だと思われてきました。

ハッキングを受けた後の危機管理活動もほぼ日常的なものとなりました。「ハッキングは誰にでも起こりうることだ」と言われることがありますが、実社会で発生している店や銀行に対する強盗に対してそのような認識を持つ人はいないでしょう。ハッキングも銀行強盗と同じように、日常的に起こるべきことではないのです。

**サイバー犯罪者との交渉は、さらなる攻撃の引き金に？**

数十年にもわたって続けられてきたランサムウェア攻撃へのこのような対応はゆっくりと終焉を迎えようとしています。犯罪者たちは、リスクを冒して、メディアが報道せざるを得ないほどの高額な身代金を要求します。さらに、最近はハッカーがガス不足を引き起こしたり、病院や食料供給を脅かしたりする事件も発生しており、アメリカ大統領すらも対応を迫られています。

ランサムウェアは政治的・金銭目的だけでなく、重要なインフラを破壊することもあります。「サイバー戦争」という言葉は注意して使わなければいけませんが、国家、企業、個人のレベルで、もっと真剣に考え始める時期に来ているのは明らかです。

私自身の考えは明確で、単純すぎるかもしれません。他の種類のハイブリッド戦争と同様に、政府外で行われるサイバー犯罪に関しては、「抑止」が唯一の解決策と考えます。すべてのハッカーを逮捕して裁判にかけようとすることは、彼らが政府に保護されていたり、直接支援を受けていたりすることもあるため、ほぼ不可能です。

ハッカーを受け入れて保護する国は、テロリストを受け入れる国と同様に扱われるべきです。ハッキングによって燃料のパイプラインを遮断することは、国家の安全保障上、燃料の爆破と同じくらい危険なことです。本当に壊滅的な出来事が起きてから、対処を始めるのでは間に合いません。早期に、そして頻繁に、サイバー攻撃に対する対応を行う必要があります。専門家によると、ロシアを拠点とする「REvil」グループは7月に[姿を消しました](https://www.washingtonpost.com/technology/2021/07/13/revil-disappears-kaseya-hack/)。彼らは恐らく、ブランド名を変えて、これまでのように私たちの警戒心が薄れるのを待っているのでしょう。

**サイバー兵器競争の実態**

先日、私は米ニューヨーク・タイムス紙のサイバーセキュリティ担当記者、ニコール・パールロス氏（Nicole Perlroth）に話を伺う機会がありました。パールロス氏は世界中のサイバー攻撃を第一線で報道している記者で、サイバー兵器戦争に関する本『This Is How They Tell Me the World Ends: The Cyberweapons Arms Race（世界の終わりはこうしてやってくる サイバー兵器開発競争）』を執筆し、今年発売されました。

どのような場合に政府が介入すべきで、民間企業に高いコストをかけずにセキュリティを向上させるには、どのような手段や規制を適用すればよいのか？また、犯罪者を攻撃する「ハッキング・バック」は非倫理的なのか？私たちが直面している脅威の本質と、それに対して何ができるか、また技術から地政学までの幅広いテーマについて議論しました。

パールロス氏によると、サイバーセキュリティ対策はアメリカの企業にとってROI（投資利益率）がないことから、強化されてきませんでした。さらに、企業におけるあらゆるプロセスがデジタル化された結果、サイバー攻撃の高度化と対象範囲の拡大も進みました。サイバー攻撃が深刻化し、身代金の要求額が高まるにつれ、ランサムウェアを支払ったほうがシステムの再構築よりは安いとは言えない状況となって、ようやく企業はサイバーセキュリティ対策の重要性を認識しはじめています。

技術的にも専門的にも多くの優位性を持っているアメリカのような国が、サイバー戦争の分野では困難を抱えていることは、悲劇とも言えます。企業が大規模なサイバー攻撃の被害を受けても、犯罪者は罰を科されることがないため、攻撃は止まることなく繰り返されています。今こそ、サイバー犯罪者に厳重な処罰を与えることを真剣に考えるべきタイミングといえるでしょう。