サイバー・テロ
日米 vs. 中国

タイトル　　サイバー･テロ　 日米 vs. 中国

著　 者　　土屋大洋（つちや もとひろ）

出 版 社　文春新書

発 売 日　2012 年 9 月 20 日

ページ数　 230p

コンピュータウィルスに感染し、PC を遠隔操作された 4 人が相次いで警察に誤認逮捕された事件は社会を震撼させた。

この事件で警察は犯罪予告文の書き込みやメール通信を行った IP アドレスから犯行に使われたパソコンを特定した。ところが、犯行に使われた機器の持ち主は犯人ではなかった。このようなウィルスはプロの犯罪者でなくても、何処にでもいる普通のプログラマーでも簡単に作成可能な時代になった。

今回の誤認逮捕は、第三者が操作した可能性について技術的確認をしなかったところに起因している。

しかし、こうした遠隔操作事件の手口はこれまでも様々な犯罪で登場しており、一般の人も無縁とは言えない時代になってきた。

本書は、国際政治学者である著者が世界中で生じた様々なサイバー攻撃の事例を丁寧に紹介している。

2006 年のブッシュ政権によるイランへのサイバー攻撃、すなわち核施設の遠心分離器を作動停止させたウィルスによる攻撃はサイバー戦争の時代の幕開けとなった。

すでに、アメリカ国防省は、陸、海、空、宇宙に次ぐ第 5 の戦闘空間としてサイバースペースを位置付けている。

さて、近年のサイバー攻撃の例を見てみよう。

2000 年 1 月：科学技術庁など政府機関サイトが改ざんされる。

2007 年 4 月：エストニアの政府機関や金融機関などに対し大規模な DDoS 攻撃（サーバーに大量の通信が集中することによりダメージを受け、一時的にサービスが出来なくなる）がかけられる。

2007 年 9 月：イスラエルがシリア国内を爆撃の際、シリア防空網操作の疑い。

2008 年：米国防総省の軍事機密を扱うネットワークがウィルスに感染し、他国のサーバーにデータが転送される。

2008 年：リトアニアとグルジアでロシアからと見られる大規模な DDoS 攻撃。

2009 年 7 月：米韓に大規模な DDoS 攻撃。

2009 年：油田情報などを標的とした、中国のグループによる「ナイト・ドラゴン」作戦。

2009 年 12 月：米グーグルなどのサービスを利用する中国や米国の人権活動家のメールが盗み見られるなど約 30 社が被害に遭う。

2010 年 6 月：イランの原発で制御系のシステムに影響するウィルス「スタックスネット」が発見される。

2010 年 9 月：尖閣諸島問題に絡み、中国から日本の政府機関などに DDoS 攻撃。

2011 年 6 月：国際通貨基金（IMF）が数か月にわたり大規模なサイバー攻撃を受けていた事実を公表。

2011 年 6 月：米 CIA（中央情報局）の公式サイトが攻撃され、利用不能に。

2012 年 7 月：財務省のコンピュータ約 120 台が長期にわたりウィルスに感染し、情報が抜き取られていた可能性が発覚。

・・・・・などです。

原子力プラントや潜水艦などを製造する、三菱重工、IHI、川崎重工などはそうした被害を受けたという事実は、企業の信用問題に直結するためなかなか公表されることはなかったが、最近になって標的型の攻撃を受けていたことを明らかにし、この情報を皮切りに、さまざまなサイバー攻撃の被害が報告されるようになった。

2012 年 12 月 1 日の読売新聞によると、宇宙航空研究開発機構（JAXA）は 11 月 30 日、男性職員のパソコン 1 台がコンピュータウィルスに感染し、来夏初打ち上げを目指して開発中の小型ロケット「イプシロン」などの技術情報が流出した可能性があると発表。この職員は「イプシロン」の技術開発を担当しており、11 月 21 日にパソコンのウィルス検出ソフトを更新したところ、ウィルスが検知されたため、ネットワークから切り離して調べ、感染が判明したという。感染が確認されたパソコンには、「イプシロン」のほか、大型ロケット「H2A」、「H2B」の技術情報も含まれており、同機構では流出の可能性と感染経路について調べているという。

アメリカや中国におけるサイバー攻撃の能力向上は、驚くべきものがあり、今ではサ

イバー攻撃の請負業は確実に広がっており、民兵と傭兵が増えているという。
サイバー攻撃が本質的にこれまでと違う点は、攻撃があったことすら分らないようにする形で相手に被害を与えられることである。成功したサイバー攻撃は、その痕跡を残さないまま、機密情報を盗んだり、相手のシステムにダメージを与えたりする。
日本政府も、サイバーセキュリティーに比較的早い段階から意識を向けていたようであるが、残念ながら最終章を読んでも進展しているとはとても思えない。
本書のタイトルを見ると「サイバー・テロ　日米　vs. 中国」とあるので、日米と中国とのサイバー戦争かと誤解しましたが、そうではなくて、先進国も途上国もみんなやってるので日本も真剣に取り組もうというものです。

さて、その中で面白かったものを 2 つほど紹介しておきましょう。
まず、海底ケーブルの話です。
日本が宇宙空間の利用をやめても宇宙空間は存在し続け、他国は宇宙空間を何の支障もなく使い続けるだろう。しかし、日本がサイバースペースから撤退すれば、サイバースペースの様相は大きく変わる。少なくとも、アメリカと東アジアの結節点となっている日米間の海底ケーブルが使えなく心配がある。
1950 年代になると通信衛星が登場したため、海底ケーブルは 1 時的に衰退するが、光ファイバーが実用化されてから、再び海底ケーブルも使えるようになった。
今では、太平洋の通信の大半は人工衛星ではなく海底ケーブルを通っていると言われている。その中で、日米間の海底ケーブルがもっとも充実している。
単位時間あたりどれくらいの情報を送ることが出来るかという伝送量から考えれば、現在では圧倒的に海底ケーブルに依存せざるを得ないと言われている。
インターネットは非同期通信なので、遅延には耐性があり、ほんのわずかな遅れが致命的というわけではない。
東日本大震災で茨城県沖の太平洋に敷設されていた海底ケーブルが多くの地点で切断された。戦時に海底ケーブルが切断された場合、相互接続しているネットワークが意図的に止められたら、あるいは特定のトラックしか流されなかったり、途中で傍受・検閲されたりしたら、どうだろうかという問題がある。

現在、日中文明が衝突していると言われる中国の取り組みはどうだろうか。ロシアに加えてアメリカ政府とアメリカ国防省が警戒しているのは中国の動向です。アメリカと中国は恒常的なサイバー戦争状態にある。
誰がサイバー攻撃を掛けているのか。何時も指をさされるのは中国とロシアである。少なからぬジャーナリストたちが中国とロシアが犯人だと断じている。とはいうものの、誰にでも分る明確な証拠は未だに示されていない。アメリカや日本に対する攻撃元となっている IP アドレスは中国になっていることをもって、中国が攻撃していると理解され

ている。

かって、中国のテレビ番組で、法輪功のウェブサイトに人民解放軍がサイバー攻撃を仕掛ける様子が実演されたという（この映像は、You Tube にも載せられ話題になった）。中国からアメリカにあるサーバーにサイバー攻撃をしていることを実演したわけだから、これは限りなく「クロ」であることを示している。

しかし、中国のコンピュータに対するサイバー攻撃では、攻撃に関与した IP アドレスのうち、日本からのものが 22.8%、アメリカからは 20.4%、韓国からは 7.1%だそうである。もっとも、このデータは「自作自演によるもの」と疑われている。

中国政府は厳しい通信検閲を実施しているわけだから、第 3 者が国外から攻撃を操作しているなら、それを探知して止めることもできるはずである。

中国からのサイバー攻撃は三つの可能性があるとしている。

第 1 に、「愛国無罪」を合言葉に、日本やアメリカへのサイバー攻撃を面白半分にやっているグループ。

第 2 に、諸外国の企業や政府から機密情報を盗もうとしている人達。中国では新しい技術を生み出すことは非常に難しいが、それを真似るのは簡単である。サイバー攻撃は安上がりな選択肢である。中国はもともと、ネット時代以前から、産業スパイは悪名高く、中国のインテリジェンス機関も経済的な利害に基づいて行動する場合が多かった。

第 3 は、国家安全保障的あるいは軍事的な意図を持ってサイバー攻撃を行う場合。

いずれにしても、中国にとってサイバー攻撃は「卑怯な手段」ではなく、「コストパーフォーマンスに優れた手段」ということになる。つまり、「ルールのある領域では思う存分破壊し、ルールのないところでは勝手にのさばる」というわけである。その矛先が日本に向いてくるのも時間の問題だろう。

本書を読んで我々一般の利用者のネット犯罪、サイバー・テロに対する意識の低さを反省させられた。日本では、サイバーセキュリティーは必ずしも魅力的な仕事とは認識されておらず、企業活動の中では「コスト」と考えられているケースが多い。

つまり、サイバースペースにおいて「安全に金を払うのはコストでしかない」というわけである。サイバーセキュリティーが重要だと何となく理解できても、それを担う人材を育成しようという機運は必ずしも強くないし、仮にそうした人材が企業の中にいたとしても厚遇されるわけではない。「出世」においても「給与」においても有利にならないどころか、むしろ「足かせ」にすらなっているというのも日本でこの分野の人材が育たない大きな理由にもなっている。

日本では、IT 技術者の社会的地位も低く、サイバー犯罪が進化しているというのに、民間で活躍している凄腕の技術者の知見を上手く利用しないという手はない。最終章でそのことに言及してはいるが色々と出来ない理由を付けて真剣に考えているとも思えない。

今後、情報通信技術を安心して利用できる環境の実現、つまりサイバーセキュリティー先進国の実現が、日本の持続的発展と情報技術を利用したより良い国民生活の実現につながるのは言うまでもない。

今のところ一般の利用者には実害は少ないようだが、一般の利用者は、サイバー・テロによる犯罪にどのように向き合えば良いのだろうか。

サイバー攻撃、サイバー・テロ、サイバー戦争は、すでに長い間、小説や映画のテーマだったが、そこでは最悪のシナリオが想定され、壊滅的な被害が起きるように描かれてきた。映画「ダイ・ハード　4.0」などは極端だが良い例ではないだろうか。

2007 年 7 月に公開された映画「ダイ・ハード　4.0」では、例によってニューヨーク市警のジョン・マクレーンの活躍を描いている。独立記念日の前夜。ワシントン DC の FBI 本部に設置されたサイバー犯罪部に異変が起こる。

交通、通信、原子力、水道などのあらゆる全米の公益事業を監視するシステムに何者かがハッキングを仕掛けてきたところから始まる、サイバー・テロをテーマにした映画である。すべてがコンピュータで動く現代社会。そこに不具合が起これば、たちまち社会機能が麻痺してしまう。

しかし、コンピュータなんか使えなくても、ちゃんと生きていけるし、人間にはもっとやるべき大切なことが山ほどあるよという映画です。

しかし、実際には、サイバー攻撃による直接の死者は、世界でもほとんど出ていない。まだ小説や映画の中の世界の話かも知れないが、それでも少しずつそれに近づいてきており、近年の様々な事例は、そうした懸念を掻き立てるものがある。

我々の社会システムがコンピュータに依存すればするほど、我々の社会はサイバー・テロからの攻撃に脆弱になることは目に見えている。

「国家安全保障」の認識に欠ける日本のサイバーセキュリティーの現実を見ていると、いま現在、日本は選挙の季節に突入しているというのに、「国家の安全保障」が選挙の争点にもならない世界でも希有な国であることを再認識する。

本書は、すでに国際政治上の課題にもなっている新しいサイバー戦争の時代を理解する上で、その「現状」、その「本質」、「今できること」などを知るにはお薦めの 1 冊です。

少し物足りない部分があるとすれば、我々一般の利用者は、サイバー・テロによる犯罪にどのように向き合えば良いのかという点についての議論が本書では置き去りにされているところだろう。

2012. 12. 1