サイバー戦争はサイバー空間での実戦

国家間のサイバー戦争は既に始まっている

ハッカー集団のバックは国の軍隊なのか ??
ハッカー集団に五輪関連機関、政府機関も狙われている
IoT デバイスなどあらゆる機器がハッキングされている

サイバー戦争という言葉がよく使われますが、まるでアニメの世界の仮想空間で行われているようでいまいちピンと来ていない人が多いのではないでしょうか？
北朝鮮が 2015 年から少なくとも 17 か国の金融機関や仮想通貨交換所に対しサイバー攻撃を仕掛け不法に 20 億ドルを超える資金を集め、核ミサイルの開発に充てているということが国連安保理事会で報告されています。もし、ある国が他国の銀行を襲って、2,000 億円を超える現金の強奪があればとんでもなく大騒ぎになるのに、サイバー攻撃だといまいち実感がありません。
ロシアの「ファンシーベア」は、「ストロンチウム」や「APT28」といった名称で知られるハッカー集団ですが、ロシア軍の情報機関であるロシア連邦軍参謀本部情報総局と通じているといわれています。このハッカー集団は、ウクライナを攻撃したり、オリンピック組織委員会、アンチ・ドーピング機関などの五輪関連機関、そして米民主党全国委員会等の政府機関へのハッキング行為を継続して仕掛けているといわれています。また、マイクロソフトは、IoT 機器のパスワードが工場出荷のままだったために、ファンシー・ベアーが標的としたネットワークに侵入できたことを複数確認していると発表しています。こうしたハッカー集団は、ネットワークにつながる IoT デバイスなど、あらゆる機器を利用して、政府機関や企業を狙って日々攻撃を仕掛けてきています。
これに対し、米国では、アメリカサイバー軍を 2018 年には統合軍として独立した軍に格上し、陸、海、空、宇宙に加えサイバー領域に対しても軍隊を強化しています。米国や北朝鮮が約 6 千人、中国が数十万人ともいわれる大規模な組織を抱えているのに対し、日本のサイバー防衛軍はまだ数百人規模です。
実際の国家間の戦争であれば、宣戦布告するのが当たり前だと思われますが、サイバー空間では、すでに宣戦布告されてしまっているのか、敵に知られないように多種多様な攻撃がすでに始まっていて、毎日のように攻防がなされています。サイバー空間では、核の制限や、生物兵器禁止条約のようなものが存在しないのか、なんでもありなすさまじい戦争が繰り広げられているようです。
現状では、サイバー防衛隊だけに頼らず、官民一体となって企業もサイバーセキュリティ対策が必要となります。