講演「迫る危機　サイバー攻撃の実態と対策」

１．国家が関与するサイバー攻撃

２０１７年５月に世界各地の病院や銀行などに悪影響を及ぼした「ワナクライ」というサイバー攻撃を覚えているだろうか？

英国の病院などのほか、日本企業にも多大な被害が確認されており、国家が関与するサイバー攻撃が一般市民に影響を与えるという代表的な例だ。ワナクライは、パソコンやサーバー内のデータを勝手に使えなくし、元に戻して欲しかったら制限時間内に「金を払え」と脅す身代金型のウイルス。金銭を支払っても、元には戻らないが、払ってしまった人も多いと報告されている。米政府は同年１２月、北朝鮮がワナクライの攻撃に関与していたと発表した。

他国のハッカーに生活を脅かされる現状が指摘される中、サイバー攻撃を盛んに他国に仕掛ける中国、ロシア、北朝鮮がどのような戦略を持っているかを知ることは非常に重要だ。

米セキュリティー専門家によると、国家の支援を受けて他国にハッキングを仕掛けるハッカー集団「**APT Advanced** Persistent Threat（高度で執拗な脅威）」は少なくとも計３８グループ存在するとされている。ＡＰＴである可能性が指摘されているグループは３００以上もある。中国については２９グループも確認されており、世界で最も多い。

２．世界を監視する中国

中国のＡＰＴの特徴は「情報の窃取」だ。他国の機密情報や技術情報を取得する攻撃が圧倒的に多い。情報を世界から吸い上げて、世界を「監視」しているのが中国のＡＰＴの傾向といえる。

最初に確認されたＡＰＴ１は上海を拠点にし、２００６年以降、米国を中心に１４１以上の企業や組織から機密情報を窃取していたとされる。米セキュリティー企業「ファイア・アイ」の専門家によると、２０１７年時点で、７つのＡＰＴが日本に攻撃を仕掛けて、情報を抜き取ろうとしていた。

手口は巧妙化しており、ウイルスを文書などとともに添付したメールを標的に送る際、ハッカーはダークウェブという企業や政府関係者のメールアドレス、個人情報が売買される闇サイトから個人情報を購入しているとされる。また、標的となる被害者が文書を開封するよう、メールの文面も不自然さを全く感じない日本語の文書であることが多くなっている。

中国は監視して収集した情報を様々な方法で生かしていく。自国の技術力と非核する研究材料にしたり、模倣して同様の技術や製品を安いコストで製造したりしている。また、諜報戦で優位に立つため、サイバー能力を駆使した偵察がどこまでできるのか試しているというケースもある。

３．情報操作するロシア

フェイクニュースなどで他国の情報を操作する一方、発電所などの重要インフラの攻撃も行うサイバー大国、ロシア。同国の攻撃は、サイバー攻撃というより、「ハイブリッド攻撃」と呼ばれることが多い。

プロパガンダやフェイクニュースによる世論操作・選挙介入、発電所などインフラ攻撃など幅広い攻撃の総称がハイブリッド攻撃と呼ばれている。最も有名な例が、２０１６年の米大統領選で民主党委員会（ＤＮＣ）のサーバーに侵入し、電子メール情報を窃取した攻撃だ。

米大統領選干渉疑惑にも触れておきたい。これは、２０１６年の米大統領選で、民主党のクリントン候補の陣営にサイバー攻撃を仕掛けメールを流出させるなど、ロシア政府が共和党のトランプ候補の陣営と共謀して選挙に干渉したとされる疑惑だ。ロシアには、コージーベアとファンシーベアという、ロシア政府から支援を受けるとされる二つのハッカー集団が存在しており、その二つのＡＰＴが、それぞれ２０１５年９月、１６年４月に民主党全国委員会のシステムに侵入し、メールを流出させたといわれている。大統領選の約１年前から用意周到に行われていた攻撃とみられている。

ロシアのＡＰＴは、ウクライナでサイバー攻撃による停電も発生させたといわれている。

私が過去に、元在日米軍司令部サイバーセキュリティー長のスコット・ジャーコフ氏を取材したところ、２０１７年時点で、中露がＡＩを使ってサイバー攻撃を仕掛ける技術を取得したとのこと。ＡＩを使用することができれば、もう人間のハッカーを多く使わなくても済む。しかも、ＡＩなら寝なくて良いので、２４時間攻撃が可能になり得る。また、人間のハッカーなら活動する時間で、追跡調査がしやすいが、ＡＩハッカーだと２４時間稼働するので、傾向を見破るのが難しくなる。この技術の利用が活発になれば、脅威になる恐れが強まる。

サイバー戦は今後、ＡＩ対ＡＩの攻防戦になると予想される。近年、イスラエルのサイバーセキュリティー企業では、ＡＩを使ってサイバー攻撃者を追跡する捜査や防衛を行う企業が増えている。守る側と攻撃する側の最新のテクノロジーを使ったいたちごっこが展開されていくと考えられる。

４．世界から金を奪う北朝鮮

北朝鮮は大変、高いサイバーセキュリティーの技術を持っているが、中国ロシアとは攻撃を行う目的が大きく異なる。経済制裁に苦しむ彼らは、多くは国が食べていくためにサイバー攻撃を仕掛けているという。

北朝鮮が支援するとされるハッカー集団の一つ「ラザルス」がこれまで関わった攻撃をみると、２０１６年２月にバングラデシュ中央銀行から８１００万ドルを盗んだ攻撃から始まり、ワナクライ、仮想通貨を盗んだ事件など金目当ての犯行が目立つ。２０１７年秋

ごろからは、ついにインターネットバンキングを利用する個人にまで攻撃を仕掛けてきた。

金正恩朝鮮労働党委員長は、「万能の剣」という言葉で表現し、サイバー戦の重要度を十分に理解している。ラザルスは「ワナクライ」事件にも関与しているとされ、米司法省がラザルスに所属していたハッカーを訴追する事態になった。海外の専門家は、北朝鮮のハッカーを「世界で最も真面目で勤勉なハッカー」と称する。それだけ、彼らは勉強熱心でエリートであり、北朝鮮では、パソコンやインターネットの熟練者は「ＩＴ人材」ではなく「サイバー戦士」と呼ぶ専門家もいる。北朝鮮には「ＩＴはビジネスや勉学のためではなく、国のために戦い他国を攻撃するためにある」という考えがあるという。

北朝鮮によるサイバー部隊の育成の歴史は、金正日氏が実権を持った後の１９８６年にさかのぼる。最初に小学生でスカウトされた選び抜かれた人材がさらに北朝鮮の「サイバー戦士養成学校」の異名を持つ金一軍事大学などで切磋琢磨する仕組み。このようなエリートが、国のために違法な金儲けをやらされているわけだ。

５．日常に忍び寄る脅威

次に、日常にどのようなサイバー脅威があるのかについて簡単に説明したい。

今は、テレビやエアコン、車などインターネットにつながる製品が多く流通している。その中で、各国のハッカー集団がインターネットを通して、こういった製品にサイバー攻撃を仕掛ける可能性が指摘されている。

まずは、スマートテレビ。市販の「スマートテレビ」の画面を停止させ、不正に金銭を要求する脅迫文を表示させるウイルスが検出され、感染被害も国内で出た。これは、ワナクライとほぼ同じ内容で、感染するとテレビ画面が停止し、代わりに画面上に法務省などを装って「ブロックを解除するためには金を払え」という表示が出る。

他にも、まだ攻撃は確認されていないが、ＡＩスピーカーに対する攻撃の可能性も指摘されている。米国では、エアコンの温度を低温状態に固定し、操作不能にする攻撃も報告されている。

６．日本の課題～東京五輪に向けた対策～

最後にこのような中国、ロシア、北朝鮮のサイバー大国に囲まれて、日本が防衛のために何をすべきなのかをまとめたい。特に、２０２０年には、東京五輪が開催され、他国のハッカーからサイバー攻撃を受ける脅威が高まる。

まず、五輪開催時にどのようなサイバー攻撃の脅威があるのか説明しよう。例えば、２０１８年２月に開催された平昌五輪では、開会式の同月９日、式を標的にしたコンピューターウイルスにより五輪会場でネットワーク障害などが発生した。 他にも、平昌五輪に関連する機関の機密情報を狙うサイバー攻撃も確認されている。五輪を狙うサイバー攻撃は今に始まったことではなく、２０１２年のロンドン五輪でも起こった。同五輪では２億回を超えるサイバー攻撃があり、開幕式で会場の電力設備を狙った攻撃が計画された。

最も懸念されているのが電力やガス、医療、水道、金融などの重要インフラへの攻撃だ。米国の専門家に取材すると、今、ネット上で、インフラを攻撃する新種のウイルスが世界で週３００～５００個も開発されているという。電力会社の担当者に話を聞くと、「もし、期間中に原発がサイバー攻撃を受けたら、五輪を中止せざるをえないほどの被害を受ける」との答えが返ってきた。政治的な理由で、五輪の中断を狙う他国のＡＰＴが攻撃を仕掛ける恐れが指摘されている。

今の段階で、日本で電力会社などのインフラを狙った大規模なサイバー攻撃は確認されていない。しかし、欧米ではこのように、ダムの制御システムや送電網ネットワークが攻撃されている。日本でも起こらないという保証はどこにもない。

このような危機が日本に目前に迫る中で、日本の課題は何なのか。

まず、セキュリティー分野の人材難。最近、日本の様々な場面で、セキュリティー人材を育てようとしている努力はみえる。しかし、それらはオペレーションを行う人材であり、実際に必要とされる、上位層の技術者を育てるに至っていないという意見は多い。また、現在の日本は、大規模なサイバー攻撃を受けた場合でも、被害や波及した影響の確定まで報告されるのに相当な時間がかかってしまっている。必要な状況把握を正しく行うために、技術を確立し、体制を整備することが求められる。

個人的に問題だと思うのは、日本ではサイバー攻撃を受けた被害者を責める風潮があることだ。米国には、サイバー業界で「ＶＩＣＴＩＭ　ＲＥＳＰＥＣＴ（被害者を尊重する）」という言葉がある。被害にあった情報を共有しやすい環境を作っていくことこそが、防衛力を最大限に高める近道だと思う。もちろん、日本を標的にする可能性のあるハッカー集団について調査し続けることも大事だ。

２０２０年まで、もう少ししかない。これだけの課題を自国だけで克服するのは不可能だ。米国土安全保障省で危機管理対策に携わったボブ・ジェンセン氏は「五輪をサイバー攻撃から守るためには１国で対応できない」と話した。米国やイスラエルなどサイバー強国との連携を進める必要があるだろう。