第1330回（2019年度 第12回）11月28日　会員セミナー

サイバーセキュリティと国際政治

国家が関与するサイバー犯罪やスパイ活動、サイバー攻撃は増え、新たな地政学・地経学・地技学上の課題となっている。サイバー空間は、国家の戦略・運営から産業・企業活動、個人の生活にまで、従来では考えられなかったレベルで大きな影響を及ぼしつつある。現状や日本が取るべき道を土屋大洋氏が語った。

講師：土屋 大洋 氏

慶應義塾大学大学院政策・メディア研究科 教授

サイバー攻撃はいつどこから仕掛けられるか分からない

サイバースペースは、深く（Deeper）、暗く（Darker）、汚い（Dirtier）という3D化が進んでいる。「ダークウエブ」（Dark Web）には特別な暗号ツールを使わないとアクセスできないが、そこでは薬物、拳銃などが簡単に買える。また、サイバー攻撃もそこに含まれる。IoTの進展、SNSの普及によってそれらを悪用する可能性が高まっている。

誰がサイバー攻撃を行っているのかを特定することをアトリビューションという。2012年10月25日、ニューヨーク・タイムズは中国の温家宝首相（当時）の不正蓄財疑惑を報道した。これに対して、上海のビルから人民解放軍の部隊によって中国がサイバー攻撃を仕掛けたという報道がされた。米国は2013年6月に行われた米中首脳会談で、中国に証拠を突きつけたが会談は決裂。翌年、米国の司法長官は、部隊の中心的な5人を特定したと発表し、顔写真を公開した。

一方、2014年12月には、映画『The Interview』に関連して、ソニー・ピクチャーズに対してサイバー攻撃が行われ、FBI長官が北朝鮮による攻撃であると特定した。サイバー攻撃はいつどこから仕掛けられるか分からない。

全ての国家にとって「工作活動」は必要なツール

サイバーセキュリティの世界には、「防衛」「攻撃」「工作活動（CNE）」という三つのキーワードがあり、特にCNEが重要になる。マイク・マッコーネル国家安全保障局（NSA）元長官は「工作活動は全ての国家にとって必要なツール」だと述べている。

例えばどういうことが行われているのか。1980年代初め、ソ連のウラジミール・ペトロフ大佐がフランス政府にソ連の工作活動に関する情報をもたらし、この情報は米国のCIAと共有された。その後、米国の国家安全保障会議（NSC）スタッフのガス・ワイスは、ソ連に意図的にパイプラインの制御ソフトを渡し、不正プログラムが仕込まれたこのソフトによってシベリアのパイプラインが大爆発を起こしたとされる。

2016年の米大統領選挙では、プーチン大統領とヒラリー・クリントンの確執を背景にロシアによる介入が行われた。これをきっかけに米国はサイバー軍を格上げし、2018年9月には国防総省が平時から他国のネットワークに入り込み攻撃を食い止める「前方防衛方針」を打ち出し、中間選挙への介入を阻止した。

また、2018年10月にはアップルとアマゾン・ウェブ・サービスが使うエレメンタル社のサーバー用マザーボードに不正チップが埋め込まれていたとの報道があった。サーバーは中国で組み立てられたもので、同社はCIA、米海軍、米国防総省などにサーバーを納入していたことから、攻撃されれば甚大な影響が及んだといわれる。

核を持たない日本は積極的にインテリジェンス強化を

サイバースペースは、陸・海・空・宇宙に続く5番目の作戦領域となっている。だが、サイバースペースは端末と通信チャンネルと記憶装置の集積で攻撃が行いやすい。特に海底ケーブルは脆弱（ぜいじゃく）である。ハワイの海底ケーブルが攻撃されれば、日本にも大きな影響が及ぶ。それだけにアトリビューションと抑止が重要な課題になる。

サイバーセキュリティはインテリジェンスの世界であり、その世界の核心はアトリビューション能力である。すでに世界各国では取り組みを進めているが、日本では憲法21条の絡みなどもあって取り組みが遅れている。安全保障とプライバシーのバランスを取りつつ、日本も積極的にインテリジェンスを強化すべきである。それこそが核を持たない日本が、今後も専守防衛を維持する方策だと考える。